Online Backup User's Guide V6.7

2011/2012 Edition

Online Backup User's Guide **V6.7**

Revision History

Date	Descriptions
5 July 2011	**Updated:** **1.3 System Requirements** **2.2 JVM (Java Virtual Machine) memory allocation** **14.1.2 Requirements and Recommendations** **14.1.4 How to backup virtual machines on VMware ESXi / ESX Server** **14.2.2 Requirements and Recommendations** **15.2 Overview** **18.1 Requirements** **Appendix B Product Documentations**
24 August 2011	**Updated:** **18.4 How to perform Brick-Level backup** **18.5 How to perform Brick-Level restore**
8 September 2011	**Updated:** **13.2 Backup virtual machines running on VMware Server** **13.2.1 Supported versions** **13.2.2 Requirements and Recommendations** **13.2.3 Limitation** **13.2.4 Overview** **13.2.5 How to backup virtual machines on VMware Server** **13.2.6 How to restore virtual machines on VMware Server** **13.3 Independent disk for VMware virtual machine**
19 September 2011	**Updated:** **15 Backup / Restore Microsoft Exchange Server** **15.1 Supported versions** **15.2 Backup Microsoft Exchange Server 2003 / 2007** **15.2.1 Requirements and recommendations** **15.2.2 Overview** **15.2.3 How to backup Microsoft Exchange Server 2003 / 2007** **15.3 Restore Microsoft Exchange Server 2003 / 2007 (installation on Windows 2003 Server)** **15.4 Backup Microsoft Exchange Server 2010** **15.5 Restore Microsoft Exchange Server 2010**
28 November 2011	**Updated:** **9 In-file Delta Technology** **9.1 Overview** **9.1.1 Block Size** **9.1.2 Apply to files (Minimum Size)** **9.1.3 Delta Merging (Enable delta merging)** **9.1.1.3 Overview** **9.1.2.3 Limitation** **9.1.3.3 Delta Merge Policy** **9.1.4.3 Delta Merging Process** **9.1.5.3 Delta Merging Example** **9.1.4 In-File Delta Type**

	9.1.1.4 Advance In-file Delta Type **9.1.5 Upload full file when** **9.1.1.5 No. of Delta** **9.1.2.5 Delta Ratio** **10 Backup / Restore Windows System State** **10.1 Supported Versions** **10.2 Requirements and Recommendations** **10.3 Overview** **10.4 How to backup Windows System State** **10.4.1 For Windows XP, 2003 / R2** **10.4.2 For Windows Server 2008 / R2, SBS 2011** **10.5 How to restore Windows System State** **10.5.1 For Windows XP, 2003 / R2** **10.5.2 For Windows 2008 / R2, SBS 2011** **10.5.3 For Windows 2008 / R2 Domain Controller** **13 Backup / Restore VMware Virtual Machines** **13.1 Backup virtual machines running on VMware ESXi / ESX Server** **13.1.1 Supported versions** **13.1.2 Requirements and Recommendations** **13.1.3 Limitation** **13.1.4 Overview** **13.1.5 How to backup virtual machines on VMware ESXi / ESX Server** **13.1.6 How to restore virtual machines on VMware ESXi / ESX Server** **14 Backup / Restore Microsoft Virtual Machines** **14.1 Backup virtual machines running on Hyper-V Server (Non-Cluster environment)** **14.1.1 Requirements and Recommendations** **14.1.2 Limitations** **14.1.3 Overview** **14.1.4 How to Backup Microsoft Virtual Machines** **14.1.5 How to Restore Microsoft Virtual Machines** **14.2 Backup virtual machines running on Hyper-V Server (Cluster environment)** **14.2.1 Requirements and Recommendations** **14.2.2 Limitations** **14.2.3 Overview** **14.2.4 How to Backup Microsoft Virtual Machines** **14.2.5 How to Restore Microsoft Virtual Machines**

Table of Contents

1 Overview 1
1.1 Conventions 1
1.2 Definitions, Acronyms and Abbreviations 1
1.3 System Requirements 2
1.4 Important Notes 2
2 Best Practices and Recommendations 3
2.1 Recommended hardware specification 3
2.2 JVM (Java Virtual Machine) memory allocation 3
2.3 Storage size for user folder of your operating system 4
2.4 Temporary directory for Quick Backup 4
2.5 Encryption 4
2.6 Backup Schedule 5
2.7 Differential and incremental In-file delta backup 5
2.8 Difference between Local Copy and Seed Load 6
2.9 Recommended backup exclusions 7
2.10 Disable SELinux (Security-Enhanced Linux) 7
2.11 Single backup user account for multiple computers 7
2.12 Consideration when using Continuous Data Protection (CDP) 8
2.13 Size of your backup source 8
2.14 Recovery plan and routine recovery test 8
3 Installing Quick Backup 10
3.1 Installing Quick Backup on Windows platforms 10
3.1.1 Installing Quick Backup 10
3.1.2 Installing Quick Backup using the command line (silent mode) 11
3.1.3 Configuring Quick Backup 12
3.2 Installing Quick Backup on Mac OS X platforms 14
3.3 Installing Quick Backup on Linux / FreeBSD / Solaris 15
3.3.1 Installing Quick Backup on Linux 15
3.3.2 Installing Quick Backup on Solaris 17
3.3.3 Installing Quick Backup on FreeBSD 20
3.4 Configure Quick Backup via X-Windows 21
3.5 Command Line Mode 24
4 Uninstalling Quick Backup 26
4.1 Uninstalling Quick Backup on Windows platforms 26
4.2 Uninstalling Quick Backup on Mac OS X platforms 26
4.3 Uninstalling Quick Backup for Linux / FreeBSD / Solaris 26
5 Using Quick Backup 28
5.1 System Tray Launcher (Windows Only) 28
5.2 Logon Dialog 29
5.3 Quick Backup Main Window 31
5.4 User Profile 34
5.5 About Quick Backup Online Backup Manager 36
5.6 Backup Log 37
5.7 Restore Log 38
6 Configure Backup Sets 39
6.1 Backup Setting 39
6.1.1 New Backup Set Wizard 41
6.1.2 General 42
6.1.3 Backup Source 45

6.1.4 Backup Schedule 47
6.1.5 Encryption 52
6.1.6 Continuous Data Protection (CDP) 56
6.1.7 In-File Delta 61
6.1.8 Retention Policy 61
6.1.9 Backup Filter 65
6.1.10 Command Line Tool 68
6.1.11 Extra Backup 69
6.1.1.11 Enable off-line backup 70
6.1.2.11 Enable System Logout Backup Reminder 71
6.1.12 Local Copy 71
6.1.13 Temporary Directory 75
6.1.14 Options 75
6.1.1.14 Temporary Directory for storing backup files 75
6.1.2.14 Follow Link 76
6.1.3.14 Enable Volume Shadow Copy 78
6.1.4.14 Transfer Block Size 80
6.1.5.14 Backup File Permission 81
6.2 Single backup account for multiple computers 81
7 Backing Up Files 82
7.1 How data are backed up 82
7.2 How to start an off-site backup 83
7.3 Seed Load backup 85
8 Restoring Files 88
8.1 How data are restored 88
8.1.1 Restore Menu 89
8.1.1.1 Filter 90
8.1.2.1 Search 92
8.1.3.1 Delete extra files 93
8.1.4.1 Follow Link 95
8.1.5.1 Resolve Link 96
8.1.6.1 Delete backed up directories and files on backup server 97
8.2 How to start a restore 98
8.2.1 Restore using the Quick Backup user interface 98
8.2.2 Restore using the web interface 102
8.2.3 Restore using Decrypt File Wizard 105
8.3 IP restriction for restore using the web interface 110
9 In-file Delta Technology 111
9.1 Overview 111
9.1.1 Block Size 114
9.1.2 Apply to files (Minimum Size) 114
9.1.3 Delta Merging (Enable delta merging) 114
9.1.1.3 Overview 115
9.1.2.3 Limitation 115
9.1.3.3 Delta Merge Policy 116
9.1.4.3 Delta Merging Process 116
9.1.5.3 Delta Merging Example 116
9.1.4 In-File Delta Type 120
9.1.1.4 Advance In-file Delta Type 121
9.1.5 Upload full file when 122

9.1.1.5 No. of Delta 123
9.1.2.5 Delta Ratio..... 123
10 Backup / Restore Windows System State..... 124
10.1 Supported Versions 124
10.2 Requirements and Recommendations..... 124
10.3 Overview..... 125
10.4 How to backup Windows System State 126
10.4.1 For Windows XP, 2003 / R2..... 126
10.4.2 For Windows Server 2008 / R2, SBS 2011..... 127
10.5 How to restore Windows System State..... 129
10.5.1 For Windows XP, 2003 / R2..... 129
10.5.2 For Windows 2008 / R2, SBS 2011 132
10.5.3 For Windows 2008 / R2 Domain Controller..... 134
11 Backup / Restore System with Microsoft Windows System Backup . 136
11.1 Requirements 136
11.2 Overview..... 137
11.3 How to backup system with Microsoft Windows System Backup..... 138
11.4 How to restore system with Microsoft Windows System Backup 143
11.5 How to perform Complete PC Restore..... 147
12 Backup / Restore Windows System with ShadowProtect 156
12.1 Requirements 156
12.2 Overview..... 156
12.3 How to backup system with ShadowProtect 157
12.4 How to restore system with ShadowProtect..... 161
13 Backup / Restore VMware Virtual Machines..... 167
13.1 Backup virtual machines running on VMware ESXi / ESX Server 167
13.1.1 Supported versions..... 167
13.1.2 Requirements and Recommendations..... 167
13.1.3 Limitation 168
13.1.4 Overview..... 168
13.1.5 How to backup virtual machines on VMware ESXi / ESX Server..... 169
13.1.6 How to restore virtual machines on VMware ESXi / ESX Server 173
13.2 Backup virtual machines running on VMware Server..... 177
13.2.1 Supported versions..... 177
13.2.2 Requirements and Recommendations..... 177
13.2.3 Limitation 178
13.2.4 Overview..... 178
13.2.5 How to backup virtual machines on VMware Server..... 178
13.2.6 How to restore virtual machines on VMware Server 182
13.3 Independent disk for VMware virtual machine 186
14 Backup / Restore Microsoft Virtual Machines 187
14.1 Backup virtual machines running on Hyper-V Server (Non-Cluster environment)..... 187
14.1.1 Requirements and Recommendations..... 187
14.1.2 Limitations..... 187
14.1.3 Overview..... 187
14.1.4 How to Backup Microsoft Virtual Machines..... 189
14.1.5 How to Restore Microsoft Virtual Machines 192
14.2 Backup virtual machines running on Hyper-V Server (Cluster environment)..... 196

14.2.1 Requirements and Recommendations ... 196
14.2.2 Limitations ... 196
14.2.3 Overview ... 197
14.2.4 How to Backup Microsoft Virtual Machines in Cluster Environment ... 198
14.2.5 How to Restore Microsoft Virtual Machines in Cluster Environment ... 201
15 Backup / Restore Microsoft Exchange Server ... 206
15.1 Supported versions ... 206
15.2 Backup Microsoft Exchange Server 2003 / 2007 ... 206
15.2.1 Requirements and recommendations ... 206
15.2.2 Overview ... 206
15.2.3 How to backup Microsoft Exchange Server 2003 / 2007 ... 207
15.3 Restore Microsoft Exchange Server 2003 / 2007 ... 212
15.4 Backup Microsoft Exchange Server 2010 ... 216
15.4.1 Requirements and recommendations ... 216
15.4.2 Overview ... 216
15.4.3 How to backup Microsoft Exchange Server 2003 / 2007 ... 216
15.5 Restore Microsoft Exchange Server 2010 ... 221
16 Brick-Level Backup/Restore Microsoft Exchange Server ... 225
16.1 Requirements ... 225
16.2 Overview ... 226
16.3 Granting Privileges ... 226
16.4 How to perform Brick-Level backup ... 230
16.5 How to perform Brick-Level restore ... 232
17 Backup/Restore Oracle Database Server ... 234
17.1 Requirements ... 234
17.2 Overview ... 237
17.3 How to backup an Oracle Database (Physical Backup) ... 238
17.4 How to restore an Oracle Database ... 245
17.5 How to restore a single tablespace ... 257
17.6 Export and Import a Database (Logical Backup) ... 262
18 Backup/Restore Microsoft SQL Server ... 264
18.1 Requirements ... 264
18.2 Overview ... 264
18.3 How to backup Microsoft SQL Server database(s) ... 265
18.4 How to restore Microsoft SQL Server database(s) ... 268
19 Backup/Restore Lotus Domino / Notes ... 274
19.1 Requirements ... 274
19.2 Overview ... 276
19.3 How to backup Lotus Domino / Notes on Windows ... 276
19.4 How to restore Lotus Domino / Notes on Windows ... 281
19.5 How to backup Lotus Domino / Notes on Linux ... 283
19.6 How to restore Lotus Domino / Notes on Linux ... 289
20 Backup/Restore MySQL Server ... 293
20.1 Requirements ... 293
20.2 Overview ... 293
20.3 How to backup MySQL server on Windows ... 293
20.4 How to backup MySQL server on Linux (command line mode) ... 298
20.5 How to restore MySQL server ... 299
21 Email Reporting ... 300
21.1 New User Report ... 300

21.2 Forgot Password Report 301
21.3 Backup Job Report 302
21.4 Setting Change Report 306
21.5 Inactive User Reminder 306
22 Web Features 308
22.1 Install Quick Backup 308
22.2 Update User Profile 309
22.3 Request Forgotten Password 311
22.4 Restore/Delete/Undelete Backup Files 311
22.5 Review Backup Jobs 312
22.6 Review Storage Statistics 315
23 Further Information 316
23.1 Contact Us 316
Appendix 317
Appendix A Supported Languages 317
Appendix B Product Documentations .....**Error! Bookmark not defined.**

1 Overview

1.1 Conventions

Convention	Descriptions	Example
Bold	**Important information**	Important: The encrypting key is independent from a backup account's password.
Italic	**Folder path or file path**	***C:\Program Files\Quick Backup***
[]	**Graphical Interface Elements**	**[Backup]**
%%	**File path in Windows format**	**%Quick Backup_HOME%**
$	**File path in Mac OS X format**	**$Quick Backup_HOME**
Italic	**Command**	***sudo ./uninstall.sh***

1.2 Definitions, Acronyms and Abbreviations

Term/Abbreviation	Definition
Quick Backup	**Quick Backup Client software**
Quick Backup Server	**Quick Backup Offsite Backup Server**
Quick Backup_HOME	**The install location of Quick Backup:** **Windows** ***C:\Program Files\Quick Backup*** **Mac OS X** ***/Applications/Quick Backup***
USERPROFILE	**The location where the operating system stores the user account information.** **Windows XP/2003** ***C:\Documents and Settings*** **Windows Vista/2008/7** ***C:\Users*** **Mac OS X** ***~/.obm***

1.3 System Requirements

Please refer to Quick Backup Help Centre Article #2165 for the system requirements of Quick Backup.

1.4 Important Notes

Images, workflow or description in this document may be different from your installation. If you are uncertain about any of the instructions provided, please contact your service provider for advices.

2 Best Practices and Recommendations

This chapter describes the best practices for your backup client application.

2.1 Recommended hardware specification

For new users, the recommended hardware specification has increased with Quick Backup version 6 because of new features such as virtual machine backup (e.g. VMware and Hyper-V), delta merge, and multi-thread implementation for backup and restore.

Quick Backup is recommended to be installed on a 64 bit machine, with multiple CPUs and cores, especially for environment setup with application specific backup module such as virtual machine, MS Exchange, or bare-metal backup.

When installing the backup client application, please thoroughly evaluate the computer's specification before the installation to ensure it meets the minimum hardware requirements and recommendations.

For existing users, the backup process may take up a higher amount of CPU and may slow down the client computer due to the multi-thread implementation since version 6. Please consider upgrading your existing client computer to cope with the higher specification demand.

2.2 JVM (Java Virtual Machine) memory allocation

For resource intensive backup modules such the following:

- MS Exchange Server backup
- MS VM backup
- MS Windows System backup
- ShadowProtect System backup
- System State backup
- VMware VM backup

If you are experiencing performance issues with the backup application, a common cause is the lack of JVM (Java Virtual Machine) memory allocated for the backup application. The default setting of the maximum heap size is 768 MB.

Consider increasing the JVM (Java Virtual Machine) memory allocation to improve performance of the backup operation. But note that the maximum memory allocated **should not** exceed **70%** of the total memory available for the system.

You can increase the maximum heap size of the application by referring to the instruction provided in Quick Backup Help Centre article #2438.

2.3 Storage size for user folder of your operating system

Your backup user profile folder (.obm) is stored under the operating system user profile location ${UserProfile}.

This folder is used for various purposes, such as storage of your backup logs, user configuration files, temporary delta file and other files of temporary nature.

Ensure that sufficient disk space is present on the partition which contains the backup user profile.

2.4 Temporary directory for Quick Backup

For backup modules such as the following:

- MS Exchange Server backup
- MS Windows System backup
- ShadowProtect System backup
- System State backup

Corresponding data are spooled to a temporary directory before they are compressed, encrypted and uploaded onto the backup server.

It is highly recommended that the temporary directory or volume used for these modules is not a system volume (e.g. not the same partition which the operating system is installed on).

It is also recommended that the temporary directory or volume configured to have at least storage space of 150% of the expected backup size.

Regular checks on the temporary directory, for left over files due to previous unsuccessful backup are also recommended.

2.5 Encryption

The encryption key is very important that it is recommended to write down, and make additional copies of the key.

Please store the key in safe location so that it is readily available when needed to restore data.

In some cases, encryption key is administrated by your service provider. Please consult your service provider for further details.

For maximum security, please select an encryption key with more than 8 characters, containing at least two of the following three character groups:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numerals (0 through 9)

If you lose the encryption key, the data is irretrievable.

2.6 Backup Schedule

In general, it is recommended that a daily backup be performed for a server or desktop. For mission critical server, a backup schedule should be configured according to the requirement of your recovery plan.

For computer with multiple backup sets configured, please configure their schedule to different time period to evenly balance the loads of the backup operation on the computer.

2.7 Differential and incremental In-file delta backup

Consider your restore requirements before setting up your In-file delta settings:

A full backup backs up all files in full, providing the fastest restore time as the restore would only require one set of data. But it is the most time-consuming, storage space-intensive and the least flexible of all three types.

A differential In-file delta backup backs up only modified parts of a file since the last full back. Differential In-file delta backup is quicker than full backup because less data are being backed up, but the amount of data being backed up grows with each differential In-file delta backup until the next full backup is performed.

An incremental In-file delta backup also backs up modified parts of a file. The difference is it only backs up the changes that occurred since the last backup, be it full, differential or incremental backup. The result is a smaller and faster backup.

While incremental backups give much greater flexibility, data backed up by long chain of incremental In-file delta backup will take a lot longer to restore, and is prone to data lost (e.g. broken delta chain).

The following table summarizes the benefits and drawbacks of the three backup types:

Type	Benefits	Drawbacks
Full	Restoration is the fastest of all three types.	Backup process is the slowest of all three types. Highest storage requirement.
Differential	Backup speed is faster than full backup. Restoration is faster than data backup with incremental In-file delta. Less storage space is need than a full backup.	Restoration is slower than data backup with full backup. Backup process is slower than incremental In-file delta backup.
Incremental	Backup process is fastest of all three types.	Restoration is the slowest of all three types.

	Least storage space is required.	Prone to data lost.

Assuming that a daily backup job is performed, the following In-file delta setting is recommended for your backup operation:

Weekday	Backup Type
Day 1	Full
Day 2	Incremental
Day 3	Incremental
Day 4	Incremental
Day 5	Differential
Day 6	Incremental
Day 7	Incremental

2.8 Difference between Local Copy and Seed Load

The Local Copy and Seed Load features are very similar in terms of what they do.

While the Local Copy feature is designed for having an extra copy of the backup data at the client site, the Seed Load feature is designed for initial backup of large data (e.g. initial backup of large MS Exchange database).

A Seed Load backup is performed onto a removable storage device to be imported on the backup server physically, bypassing the bottleneck of Internet backup.

The major differences between Local Copy and Seed Load are:

Feature	Local Copy	Seed Load
Retention Policy	Retention policy can be applied on local copy backup.	No retention policy is applied on seed load backup.
In-file Delta	Advance In-file Delta type setting can be applied on local copy backup.	No In-file Delta type setting is applied on seed load backup.
Backup Schedule	Local copy backup can be performed manually or by schedule.	Seed load backup can only be performed manually.

For performance consideration, it is highly recommended that the local copy backup be performed on a local hard disk, and not to a network location.

2.9 Recommended backup exclusions

Backing up system, system cache, redundant or non-essential files, such as Windows page file can cause unnecessarily high data change rates and excessive use of network bandwidth, affecting backup operations negatively.

Consider excluding the following files when configuring your backup source location.

Operating system	Directory path
Windows	C:\hiberfil.sys C:\Pagefile.sys C:\Program Files* C:\RECYCLER C:\System Volume Information C:\Windows* ${App_Data}\Avg7 ${App_Data}\Avg8 ${App_Data}\Kaspersky Lab ${App_Data}\McAfee ${App_Data}\McAfee.com ${App_Data}\Microsoft ${App_Data}\Sophos ${App_Data}\Symantec **.tmp *\Application Data\Macromedia* *\Application Data\Mozilla* *\Local Settings\Application Data\Microsoft* *\ntuser.dat
Linux	/dev /lost+found /proc /sys /tmp /var/empty /var/lock /var/run /var/spool /var/tmp

2.10 Disable SELinux (Security-Enhanced Linux)

For backup client installation on Linux, it is recommended to disable the SELinux (Security-Enhanced Linux) feature to avoid error during your backup operation.

2.11 Single backup user account for multiple computers

For backup of multiple computers with a single account, separate backup set for each computer must be created, because backup set cannot be shared for multiple computers.

For administrative concerns and considerations (e.g. data lost due to incorrect configuration), it is not recommended that a backup user account to have more than 10 backup sets for backup of multiple computers.

Incorrect configuration can lead to data lost.

2.12 Consideration when using Continuous Data Protection (CDP)

Some advantages of using CDP include:

1. CDP prevents loss of data as the modified contents of the files are backed up automatically in close to real-time.

2. Frequently modified data is backed up in almost real-time. Thus, you can accurately restore an earlier version created on the same day.

Although CDP can be a helpful feature, the protection offered by CDP is often heralded without consideration of the disadvantages that it can present. Specifically, the continuous CPU, memory and bandwidth usage can adversely affect the corresponding machine's performance.

Please consider the limitations imposed by CDP before utilizing such feature.

CDP is not a replacement for traditional schedule backup but is a complimentary backup, which works along with the scheduled backup to provide timely protection for your data.

2.13 Size of your backup source

The total number of files selected as backup source and the relative size of each file impacts backup performance. Fastest backups occur when the source contains fewer large size files, while slowest backups occur when the source contains millions of small files.

For backup set with huge amount of files, please consider splitting the set into multiple sets with smaller source to improve the speed of the backup operation.

2.14 Recovery plan and routine recovery test

Consider performing routine recovery test to ensure your backup is setup and performed properly. Performing recovery test can also help identify potential issues or gaps in your recovery plan.

For best result, it is recommended that you keep the test as close as possible to a real situation. Often times when a recovery test is to take place, administrators will plan for the test (e.g. reconfigure the test environments, restoring certain data in advance). For real recovery situation, you will not get a chance to do that.

It's important that you do not try to make the test easier, as the objective of a successful test is not to demonstrate that everything is flawless. There might be flaws identified in the plan throughout the test and it is important to identify those flaws.

3 Installing Quick Backup

This chapter describes how to install the backup client application.

3.1 Installing Quick Backup on Windows platforms

There are two installation methods available:

- Method 1 - Use the Installation Wizard, which guides you through the installation process.
- Method 2 - Use the command line, which is called Silent Mode Installation.

3.1.1 Installing Quick Backup

1. Download the Quick Backup installer (obm-win.exe) from the Quick Backup Server web interface.

Step 1: Download and Install
Click the below icon to download our Quick Backup software. Run the downloaded file and follow the prompts to install on your computer.
Windows 7 / XP / 2003 / Vista
Download
Linux / Ubuntu / FreeBSD
Download
Mac OSX
Download
Netware 5.1 and above
Download

2. Follow the instructions provided by Installation Wizard to complete the installation.
3. When completed, a system tray icon for Quick Backup will be installed, and Quick Backup will be launched automatically.

3.1.2 Installing Quick Backup using the command line (silent mode)

1. Download the Quick Backup installer (obm-win.exe) from the Quick Backup Server web interface.

Step 1: Download and Install
Click the below icon to download our Quick Backup software. Run the downloaded file and follow the prompts to install on your computer.
Windows 7 / XP / 2003 / Vista
Download
Linux / Ubuntu / FreeBSD
Download
Mac OSX
Download
Netware 5.1 and above
Download

2. Open a Windows command prompt (with an administrative user account on the machine).

3. Change to the directory containing the obm-win.exe file.

Type in *obm-win.exe* and the appropriate switches, for example:

```
>obm-win.exe /VERYSILENT /LANG=en /TASKS="Everyone"
```

Syntax:
obm-win.exe [{/SILENT | /VERYSILENT}] [{/LANG=xx}] [{/TASK="option"}]

Parameter	Description
/SILENT	**Install the backup application showing the installation process.**
/VERYSILENT	**Install the backup application hiding the installation process.**
/LANG=xx	**Install the backup application in the language**

	Selected.
/TASK="option"	**Install the backup application available to all users or one user only (e.g. me only).**

Value	Description
xx	**Abbreviations of the language to install the backup application in (e.g. en, it, fr).**
option	**Everyone or MeOnly.**

4. Press Enter.

3.1.3 Configuring Quick Backup

1. Launch the Quick Backup user interface by double-clicking on the desktop icon.
2. Enter the backup server hostname in the [Backup Server] field.
3. Optional - For machine that requires Internet connection through proxy, select the [Use proxy to access the backup server] option, and fill in the settings within the [Proxy setting] section
4. Press the [Next] button afterward.
5. Optional - If you do not have a backup user account, you can register for a trial user account with the following steps:
   - Enter the [Login Name] and [Password] of your choice.
   - Enter your [Email] address in the textbox provided.
   - Press the [Submit] button.
6. If you already have a backup user account, select [Already a user?] and logon to the server with your existing login credentials.
7. For first time login, you will be guided to create a backup set:
   - Select the [Backup Source] for the backup set.
   - Configure a backup schedule for unattended backups.
   - Select an encryption setting for your backup set.
   - Accept the default encryption settings (using the backup user account's password string as encrypting key) if no change are necessary.

Important:

Even with the default encryption setting selected, the encryption key is independent from a backup account's password.

Since encryption settings are set at a backup set's creation time, even if the password is changed afterward, the encryption key remain the same.

It is VERY IMPORTANT that the encryption key is written down, and additional copies of the key are made, and stored in safe places so that it is readily available when needed to restore data.

If you lose the encryption key, the data is irretrievable.

- Press the [OK] button to complete the configuration of backup set.
- Scheduled backup will run automatically if you leave your computer on.

8. To perform a backup immediately, click [Backup] button on the left panel.
9. Setup is now completed.

3.2 Installing Quick Backup on Mac OS X platforms

1. Download the Quick Backup installer (obm-mac.zip) from the website.

Step 1: Download and Install
Click the below icon to download our Quick Backup software. Run the downloaded file and follow the prompts to install on your computer.
Windows 7 / XP / 2003 / Vista
Download
Linux / Ubuntu / FreeBSD
Download
Mac OSX
Download
Netware 5.1 and above
Download

2. Expand the archive and execute the Quick Backup package.
3. Follow the instructions provided by Installation Wizard to complete the installation.
4. Launch the Quick Backup user interface by double-clicking on the desktop icon.
5. Enter the backup server hostname in the [Backup Server] field.
6. Optional - For machine that requires Internet connection through proxy, select the [Use proxy to access the backup server] option, and fill in the settings within the [Proxy setting] section
7. Press [Next] afterward.
8. Optional - If you do not have an backup user account, you can register for a trial user account with the following steps:
    - Enter the [Login Name] and [Password] of your choice.

      Note: Minimum length of the password is 6 characters
    - Enter your [Email] address in the textbox provided.
    - Press the [Submit] button.

9. If you have a backup user account already, select [Already a user?] and logon to the server with your existing login credentials.

10. For first time login, you will be guided to create a backup set:

    - Enter a backup set name and select the backup module type.
    - Assuming that is a file backup set, select the [Backup Source] for the backup set.
    - Configure a backup schedule for unattended backups.
    - Select an encryption setting for your backup set.
    - Accept the default encryption settings (using the backup user account's password string as encrypting key) if no change is necessary.

    Important:
    Even with the default encryption setting selected, the encryption key is independent from a backup account's password.

    Since encryption settings are set at a backup set's creation time, even if the password is changed afterward, the encryption key remain the same.

    It is VERY IMPORTANT that the encryption key is written down, and additional copies of the key are made, and stored in safe places so that it is readily available when needed to restore data.

    If you lose the encryption key, the data is irretrievable.

    - Press the [OK] button to complete the configuration of backup set.
    - Scheduled backup will run automatically if you leave your computer on.

11. To perform a backup immediately, click [Backup] button on the left panel.

12. Setup is now completed.

*For further details of each step, please refer to the following chapters.

3.3 Installing Quick Backup on Linux / FreeBSD / Solaris

3.3.1 Installing Quick Backup on Linux

1. Download the Quick Backup tarball release (obm-nix.tar.gz) from the Quick Backup Server web console.

Step 1: Download and Install
Click the below icon to download our Quick Backup software. Run the downloaded file and follow the prompts to install on your computer.
Windows 7 / XP / 2003 / Vista
Download
Linux / Ubuntu / FreeBSD
Download
Mac OSX
Download
Netware 5.1 and above
Download

2. Logon as root user in the Linux machine.

3. Create a new $Quick Backup_HOME directory (e.g. /usr/local/obm):

```
# mkdir –p /usr/local/obm
```

4. Unpack the install package to $Quick Backup_HOME:

```
# cd /usr/local/obm
# gunzip obm-nix.tar.gz
# tar –xf obm-nix.tar
```

5. For custom JRE - Install JRE v1.6 or above, and make note of the JRE installation path (e.g. /usr/java).

   - Create a symbolic link for JRE:

```
# ln –sf /usr/java /usr/local/obm/jvm
```

   - Set the $JAVA_HOME environment variable:

```
# export JAVA_HOME=/usr/java
```

   Note: Custom Java Runtime (JRE) for Quick Backup installation is only required when the client machine is not running on x86 or x64.

6. Install Quick Backup and its related services by using the following commands:

```
# cd /usr/local/obm
# ./bin/install.sh > install.log
```

   Details of the installation can be found under the install.log file in $Quick Backup_HOME/bin.

3.3.2 Installing Quick Backup on Solaris

1. Download the Quick Backup tarball release (obm-nix.tar.gz) from the Quick Backup Server web console.

Step 1: Download and Install
Click the below icon to download our Quick Backup software. Run the downloaded file and follow the prompts to install on your computer.
Windows 7 / XP / 2003 / Vista
Download
Linux / Ubuntu / FreeBSD
Download
Mac OSX
Download
Netware 5.1 and above
Download

2. Logon as root user in the Solaris machine.

3. Install the SUNWgtar package from the Solaris Installation Media which contain the GNU tar util.

4. Create a new $Quick Backup_HOME directory (e.g. /usr/local/obm):

```
# mkdir –p /usr/local/obm
```

5. Unpack the install package to $Quick Backup_HOME:

```
# cd /usr/local/obm
# gtar –zxf obm-nix.tar.gz
```

6. Remove the bundled Java JRE:

```
# rm –rf /usr/local/obm/jre32
# rm –rf /usr/local/obm/jre64
```

7. Install JRE v1.6 or above, and make note of the JRE installation path (e.g. /usr/java).

8. Create a symbolic link for JRE:

```
# ln –s /usr/java /usr/local/obm/jvm
```

9. Set the $JAVA_HOME environment variable:

```
# JAVA_HOME=/usr/java;export JAVA_HOME
```

10. Install Quick Backup and its related services by using the following commands:

```
# cd /usr/local/obm
# ./bin/install.sh > install.log
```

Details of the installation can be found under the install.log file in $Quick Backup_HOME/bin.

3.3.3 Installing Quick Backup on FreeBSD

Note that the following steps assumed that Diablo JRE 1.6.0 is already installed.

Diablo JRE 1.6.0 can be downloaded from:
http://www.freebsdfoundation.org/downloads/java.shtml

1. Download the Quick Backup tarball release (obm-nix.tar.gz) from the Quick Backup Server web console.

Step 1: Download and Install
Click the below icon to download our Quick Backup software. Run the downloaded file and follow the prompts to install on your computer.
Windows 7 / XP / 2003 / Vista
Download
Linux / Ubuntu / FreeBSD
Download
Mac OSX
Download
Netware 5.1 and above
Download

2. Logon as root user in the FreeBSD machine.

3. Create a new $Quick Backup-Home directory (e.g. /usr/local/obm):

```
# mkdir –p /usr/local/obm
```

4. Unpack the install package to $Quick Backup-Home:

```
# cd /usr/local/obm
# gunzip obm-nix.tar.gz
# tar –xf obm-nix.tar
```

5. Remove the bundled Java JRE:

```
# rm –rf /usr/local/obm/jre32
# rm –rf /usr/local/obm/jre64
```

6. Create a symbolic link for JRE:

```
# ln –sf "/usr/local/diablo-jre1.6.0" "/usr/local/obm/jvm"
```

If you are using csh shell, you need to type *rehash* and hit [Enter] for the symbolic link to take effect.

For other shell, please use the following command:

```
# setenv JAVA_HOME "/usr/local/diablo-jre1.6.0"
```

7. Install Quick Backup and its related services by using the following commands:

```
# cd /usr/local/obm
# ./bin/install.sh > install.log
```

Details of the installation can be found under the install.log file in $Quick Backup_HOME/bin.

8. Enable the backup scheduler and auto upgrade services at machine startup by adding the following entries in the system file */etc/rc.conf*:

```
obmaua_enable="YES"
obmscheduler_enable="YES"
```

Run the following scripts:

```
# /usr/local/etc/rc.d/obmscheduler start &
# /usr/local/etc/rc.d/obmaua start &
```

3.4 Configure Quick Backup via X-Windows

1. Set the DISPLAY environment variables.

sh, bash:

```
DISPLAY=IP_ADDRESS_OF_XTERMINAL[:0.0]; export DISPLAY
```

For example:

```
DISPLAY=:0.0; export DISPLAY
or DISPLAY=127.0.0.1; export DISPLAY
or DISPLAY=127.0.0.1:0.0; export DISPLAY
or DISPLAY=192.168.0.2; export DISPLAY
or DISPLAY=192.168.0.2:0.0; export DISPLAY
```

csh:

```
# setenv DISPLAY IP_ADDRESS_OF_XTERMINAL[:0.0]
```

For example:

```
setenv DISPLAY :0.0
or setenv DISPLAY 127.0.0.1
or setenv DISPLAY 127.0.0.1:0.0
or setenv DISPLAY 192.168.0.2
or setenv DISPLAY 192.168.0.2:0.0
```

2. Launch the Quick Backup user interface.

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

3. Enter the backup server hostname in the [Backup Server] field.
4. Optional - For machine that requires Internet connection through proxy, select the [Use proxy to access the backup server] option, and fill in the [Proxy setting] section.
5. Press [Next] afterward
6. Optional - If you do not have an backup user account, you can register for a trial user account with the following steps:
   - Enter the [Login Name] and [Password] of your choice.

     Note: Minimum length of the password is 6 characters
   - Enter your [Email] address in the textbox provided.

- Press the [Submit] button.

7. If you have a backup user account already, select [Already a user?] and logon to the server with your existing login credentials.

8. For first time login, you will be guided to create a backup set:

   - Select the [Backup Source] for the backup set.
   - Configure a backup schedule for unattended backups.
   - Select an encryption setting for your backup set.
   - Accept the default encryption settings (using the backup user account's password string as encrypting key) if no change is necessary.

   Important:
   Even with the default encryption setting selected, the encryption key is independent from a backup account's password.

   Since encryption settings are set at a backup set's creation time, even if the password is changed afterward, the encryption key remain the same.

   It is VERY IMPORTANT that the encryption key is written down, and additional copies of the key are made, and stored in safe places so that it is readily available when needed to restore data.

   If you lose the encryption key, the data is irretrievable.

   - Press the [OK] button to complete the configuration of backup set.
   - Scheduled backup will run automatically if you leave your computer on.

9. To perform a backup immediately, click [Backup] button on the left panel.

10. Setup is now completed.

*For further details of each step, please refer to the following chapters..

3.5 Command Line Mode

1. Backup set cannot be created in command line mode.

   Before accessing the backup application in command line mode, please use the web interface to create the initial backup set:

   - Login to the web interface.
   - To **create** the initial backup set:
     - Select the [Backup Set] tab, and [Add].
     - Select the corresponding backup type, and [Update].
     - Configure the backup set by entering the corresponding information in the available fields (e.g. Backup set name, backup source, backup schedule).
     - Click [Update] when complete.
   - To **modify** an existing backup set.
     - Select the [Backup Set] tab, and the corresponding set from the [Backup Set] drop down menu.
     - Modify the backup set setting as required.
     - Click [Update] when complete.
   - To **remove** an existing backup set:
     - Select the [Backup Set] tab, and the corresponding set from the [Backup Set] drop down menu.
     - Click [Remove]

2. Access the backup application in command line mode with the Backup Configurator:

```
# sh /usr/local/obm/bin/Configurator.sh
```

3. Enter the login credentials, backup server URL, connection protocol, and proxy settings as requested:

```
Login Name: Username
Password: ******************************
Backup Server URL: backup.server.com
Which Protocol? (1)Http (2) Https: 1
Use proxy? (Y)es or (N)o: Y
Proxy Type? (1)Http/Https Proxy (2) SOCKS: 1
Enter proxy server: proxy.server.com
```

```
Enter proxy port: 123
Enter proxy username (optional): username
Enter proxy password (optional): **********
```

4. Configure the encryption setting and schedule setting (e.g. if the backup set should run on this computer) of the initial or a newly created backup set as requests:

```
Found new backup set 'BackupSetName'
Please enter the following values for this backup set:

Encrypting Algorithm?
(1) Twofish (2) AES (3) Triple DES (4) No Encryption: 1
Encrypting Key: **********
Re-Enter Encrypting Key: **********
Encrypting Mode? (1)ECB (2) CBC: 1
Run scheduled backup on this computer? (Y)es or (N)o: Y
```

5. The Backup Configurator can also be used to modify configuration settings of existing backup set:

```
Main Menu:
----------
(1). List Backup Setting
(2). Change Password
(3). Change Network Setting
(4). Change run scheduled backup setting
(5). Toggle Masked Field (Password, Encryption Key)
(6). Generate Configuration Report (text format)
(7). Quit

Your Choice:
```

6. To perform a backup immediately, execute the command below.

```
# sh /usr/local/obm/bin/RunBackupSet.sh [BackupSetName]
```

7. Setup is now completed.

*For further details of each step, please refer to the following chapters.

4 Uninstalling Quick Backup

This chapter describes how to uninstall the backup client application.

4.1 Uninstalling Quick Backup on Windows platforms

1. On the Windows machine with Quick Backup installed.
2. Open Start menu, select [Control Panel] and [Add or Remove Programs].
3. Select [Quick Backup Online Backup Manager] from the list and press the [Remove] button.

4.2 Uninstalling Quick Backup on Mac OS X platforms

1. On the Mac OS X machine with Quick Backup installed.
2. Remove all program files by running the following command in terminal

```
>cd $Quick Backup_HOME/bin
>sudo ./uninstall.sh
```

3. Remove all backup setting files by running the following command in terminal:

```
>rm -rf ~/.obm
```

4.3 Uninstalling Quick Backup for Linux / FreeBSD / Solaris

1. On the machine with Quick Backup installed.
2. Uninstall the backup application by running the uninstall scripts

```
# sh /usr/local/obm/bin/uninstall.sh
```

3. Remove all installation files by running the following command:

```
# rm –rf /usr/local/obm
```

4. Remove all backup setting files by running the following command:

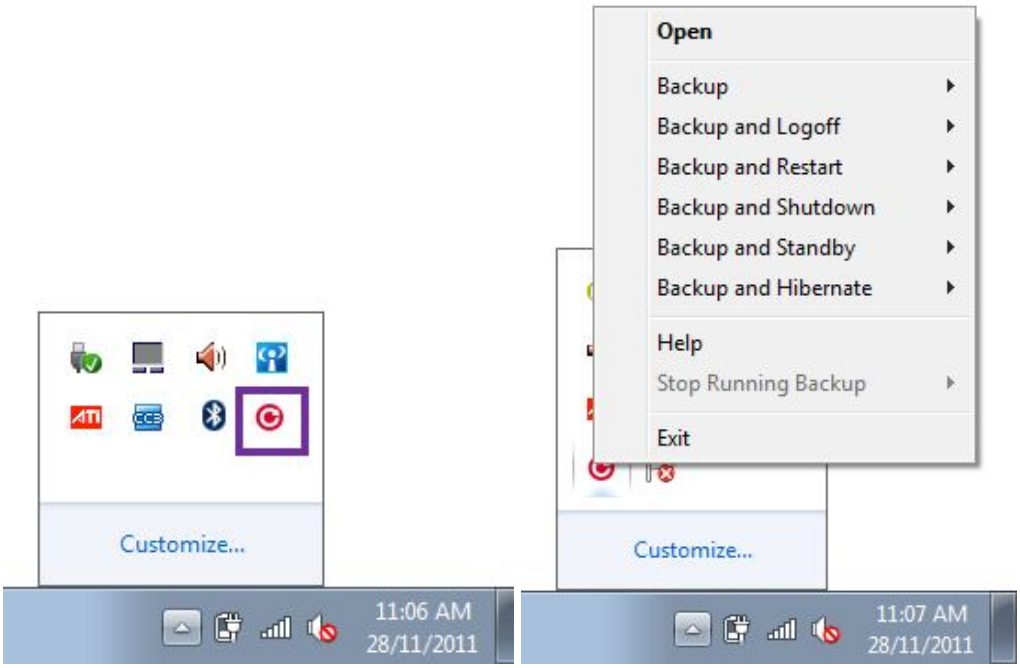
```
# rm –rf ~/.obm
```

5 Using Quick Backup

This chapter describes the various features available in the backup client application.

5.1 System Tray Launcher (Windows Only)

After a successful installation of Quick Backup, a system tray icon will be installed, and displayed under the Windows system tray area.



Right clicking on the Quick Backup system tray icon will display a menu, providing the following functions:

Menu Item	Description
Open	**Click to open Quick Backup's logon dialog.**
Backup	**Click to perform backup for a specific backup set in silent background mode.**
Backup and Logoff	**Click to perform backup for a specific backup set in silent background mode and logoff from Windows when the job is completed.**
Backup and Restart	**Click to perform backup for a specific backup set in silent background mode and restart Windows when the job is completed.**
Backup and Shutdown	**Click to perform backup for a specific backup set in silent background mode and shutdown Windows when the job is completed.**
Backup and Standby	**Click to perform backup for a specific backup set in silent background mode and enter the Standby mode**

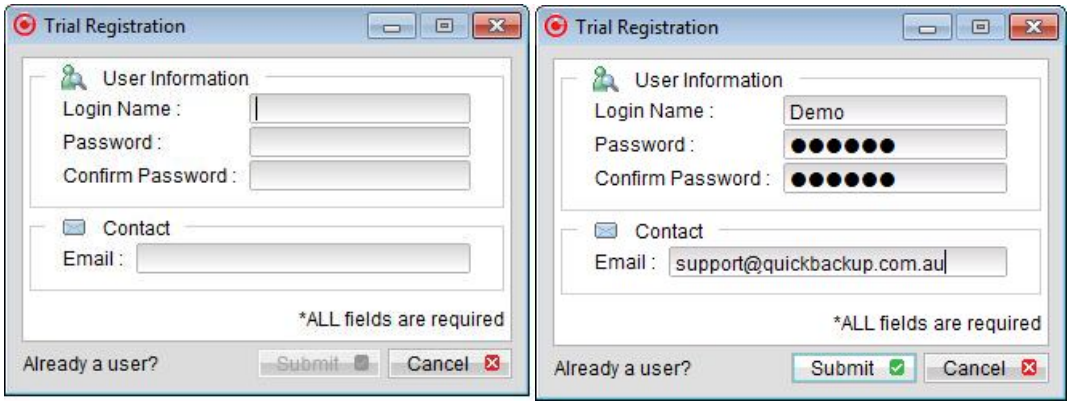
	of Windows when the job is completed.
Backup and Hibernate	**Click to perform backup for a specific backup set in silent background mode and enter the Hibernate mode of Windows when the job is completed**
Help	**Open the help dialog.**
Stop running backup	**Click to stop a running backup job chosen from the sub-menu.**
Exit	**Click to closes this system tray launcher application.**

*The availability of options listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

5.2 Logon Dialog

Double-click on the application desktop icon or system tray icon to open the logon dialog or trial registration dialog.

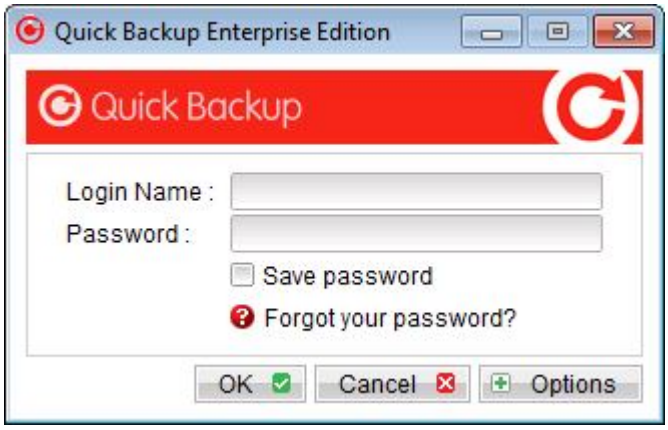
For initial login, the trial registration dialog will be displayed.



Menu Item	Description
Login Name	**Input box for entering trial backup user login name.**
Password	**Input box for entering trial backup user password.**
Contact	**Input box for entering trail backup user email contact.**
Submit	**Click to create the trial backup user account.**
Already a user?	**Click to access the login dialog, for user with backup user account already.**

*The availability of options listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

For sub-sequence login, the login dialog will be displayed.



Menu Item	Description
Login Name	**Input box for entering backup user account login name.**
Password	**Input box for entering backup user account password.**
Save password	**Checkbox to enable or disable password saving.**
Forgot your password?	**Click to request for lost password.**
Options	**Click to access advance option such as [Language], [Backup Server] and [Proxy Setting].**
Language	**Drop down menu for selecting language to start the backup application.**

*The availability of options listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Press the [Option] button to access the [Language], and [Proxy setting] settings.

Enter your login credentials in the [Login Name] and [Password] fields.

If you do not remember your password, press the [Forgot your password?] button to retrieve a forgotten password email.

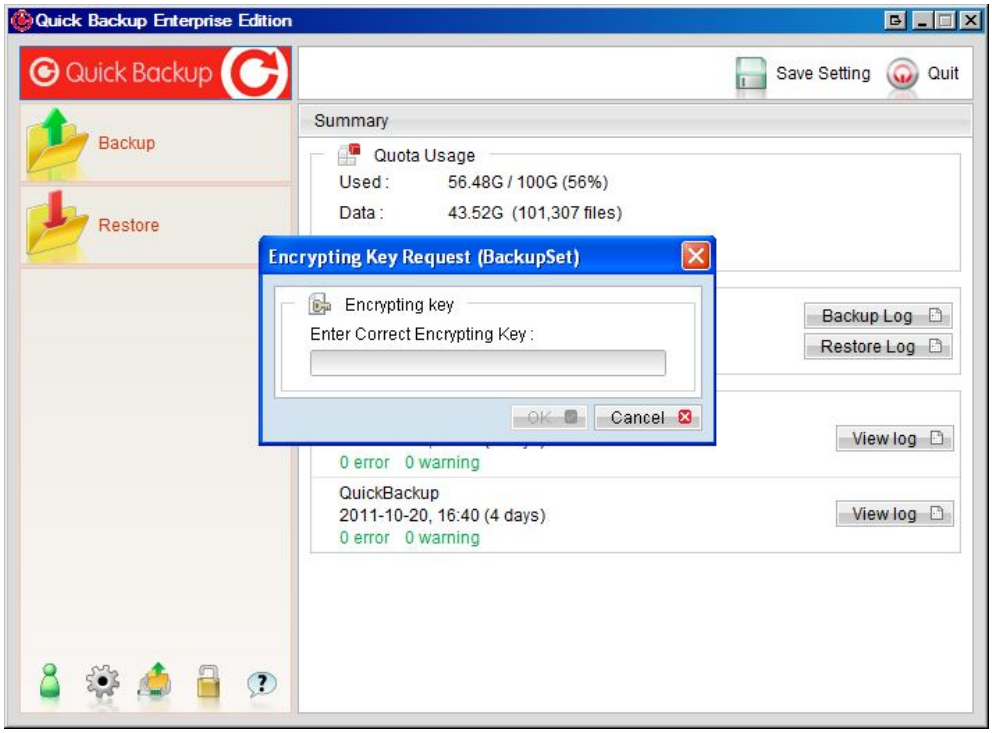
Please do not attempt to login with an incorrect password, as a backup user account will be locked after 3 bad password attempts. Backup job cannot be run for backup user account with status as locked.

Please contact Quick Backup support Phone (02) 8094 1245 or email support@quickbackup.com.au to unlock your account if it is locked.

To enable [Proxy setting], select the [Use proxy to access the backup server] checkbox button, and enter the corresponding proxy information. For [Sock] proxy, both v4 and v5 without user authentication are supported.

Press [OK] to login when all configurations are entered.

For initial login of existing backup user on new computer, you will be prompted for the encrypting key of all existing backup set.



Menu Item	Description
Enter Correct Encrypting Key	**Input box for entering encrypting key of existing backup set.**
OK	**Click to confirm on encrypting key.**
Cancel	**Click to proceed without using encrypting key.**

Enter the correct encrypting key and click [OK] to proceed.

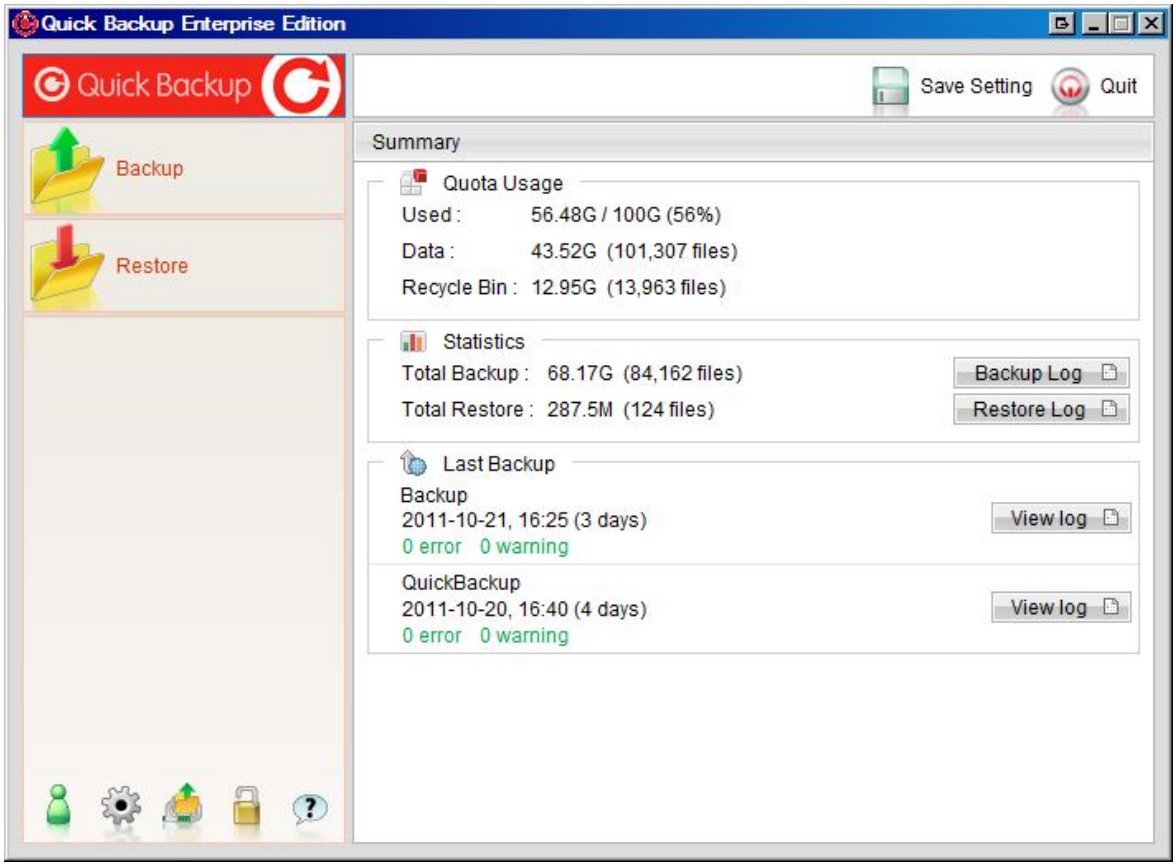
Alternatively, if the encrypting key is lost, press [Cancel] to proceed without encryption (e.g. for all backup job performed afterward).

This would allow data backed up in the future to be restore-able (as they are no longer encrypted), but existing data that are already encrypted by the lost encrypting key would not be restore-able.

In case of encrypting key lost, it is strongly recommended that a new backup set be created, to ensure that data backed up in the future is encrypted and restore-able.

5.3 Quick Backup Main Window

The main window will be displayed after a successful login.



Icon	Menu Item	Description
	Backup	**Click to perform backup for an existing backup set.**
	Restore	**Click to access the restore menu, for restoring backed up data.**
	Save Setting	**Click to save settings.**
	Quit	**Click to exit out of the backup application.**
	User Profile	**Click to access the user profile menu.**
	Backup Setting	**Click to access the backup setting menu.**
	Decrypt Local Copy Wizard	**Click to access the decrypt local copy wizard.**
	Decrypt File Wizard	**Click to access the decrypt file wizard.**

	About Quick Backup	**Click to access the About Quick Backup dialog.**
	Backup Log	**Click to view previous backup log.**
	Restore Log	**Click to view previous restore log.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

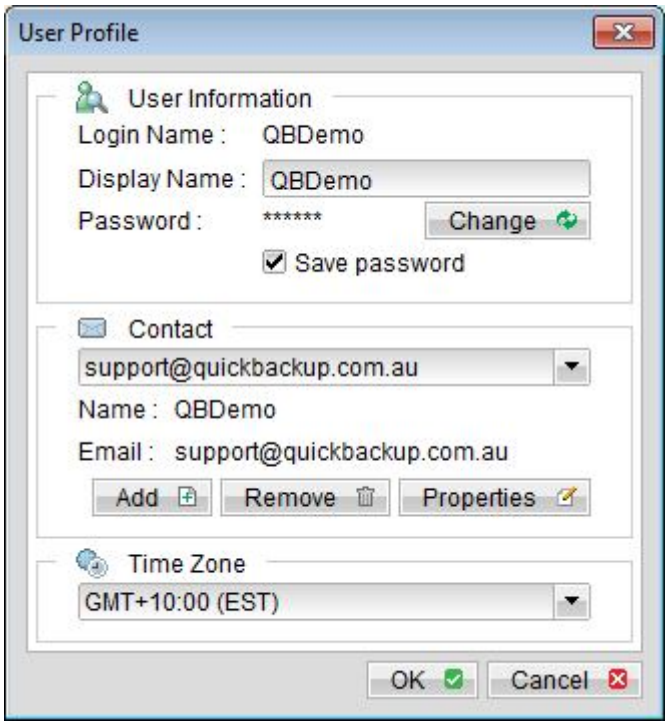
Click on the [Backup] button to perform a backup for an existing backup set.

Click on the [Restore] button to restore backed up data from the backup server to the client machine.

Other options will be discussed in the following chapters.

5.4 User Profile

To access the user profile dialog, click on the [User Profile] button at the application's main window.



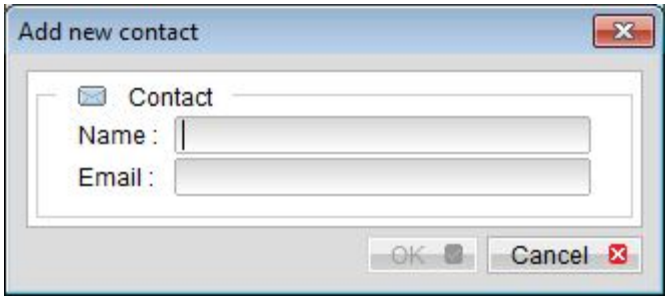
Menu Item	Description
Display Name	**Input box for entering alias of the backup user account.**
Change	**Click to access the change password dialog.**
Save password	**Checkbox to enable or disable password saving.**
Add	**Click to add contact information.**
Remove	**Click to remove contact information.**
Properties	**Click to edit existing contact information.**
Name	**Input box for entering contact name of the backup user account.**
Email	**Input box for entering contact email address of the backup user account.**
Time Zone	**Dropdown menu for time zone setting.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

You can change the backup user account's password, by pressing the [Change] button. A change password dialog will be displayed afterward.

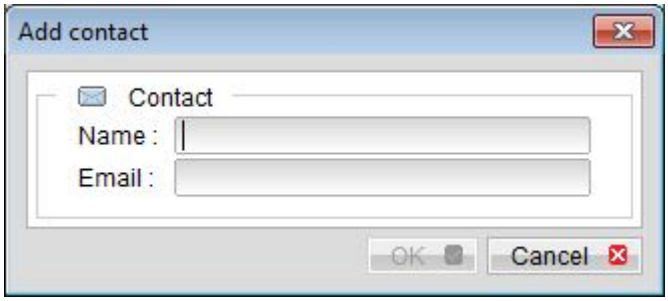
Enter your [Old Password] (e.g. existing password) and [New Password] into the corresponding textbox and press [OK].

To add new contact information for the backup user account, select [Add] to open the [Add new contact] dialog.



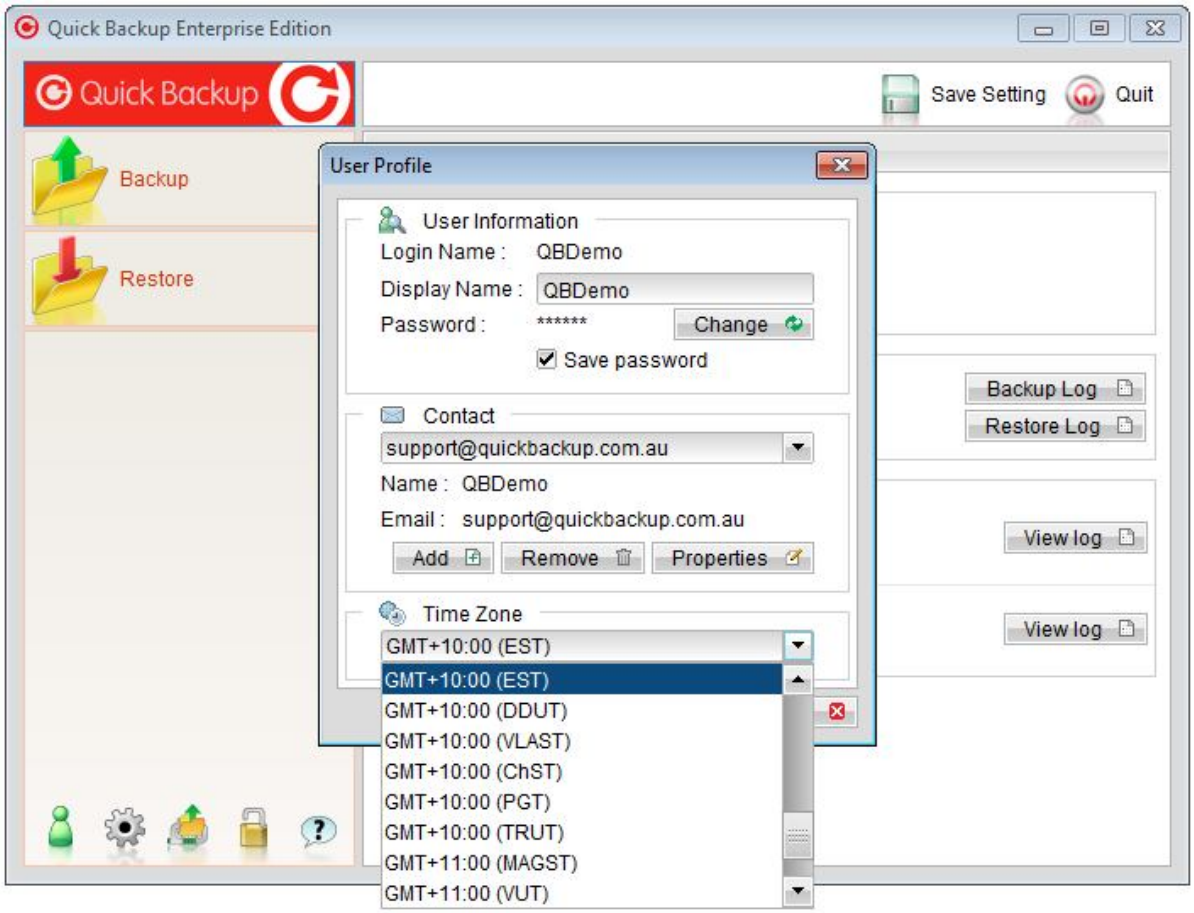
Enter the corresponding information such as [Name] and [Email] in the corresponding field, and press [OK].

To update existing contact of the backup user account, select the corresponding contact from the [Contact] drop down menu, and select [Properties].



To delete existing contact of the backup user account, select the corresponding contact from the [Contact] drop down menu, and select [Remove].

To change the backup user account's time zone setting, select the corresponding time zone from the [Time Zone] drop down menu.

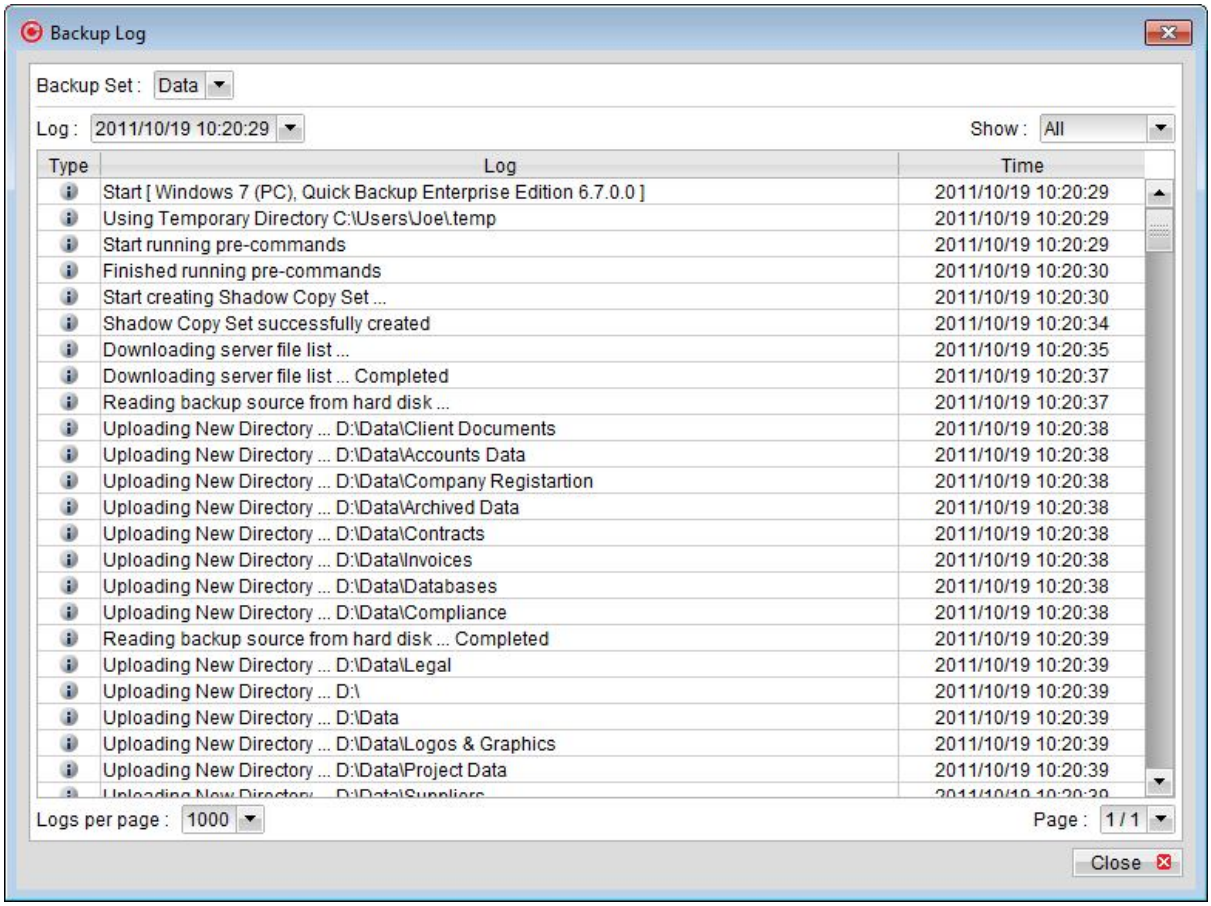


5.5 About Quick Backup Online Backup Manager

Click on the [About Quick Backup Online Backup Manager] button to view information of your backup application, such as the application version, and backup service provider's information like company name, website, email address and server hostname or IP address.

5.6 Backup Log

All backup activities are logged to a corresponding log files. To review them, click on the [Backup Log] button.

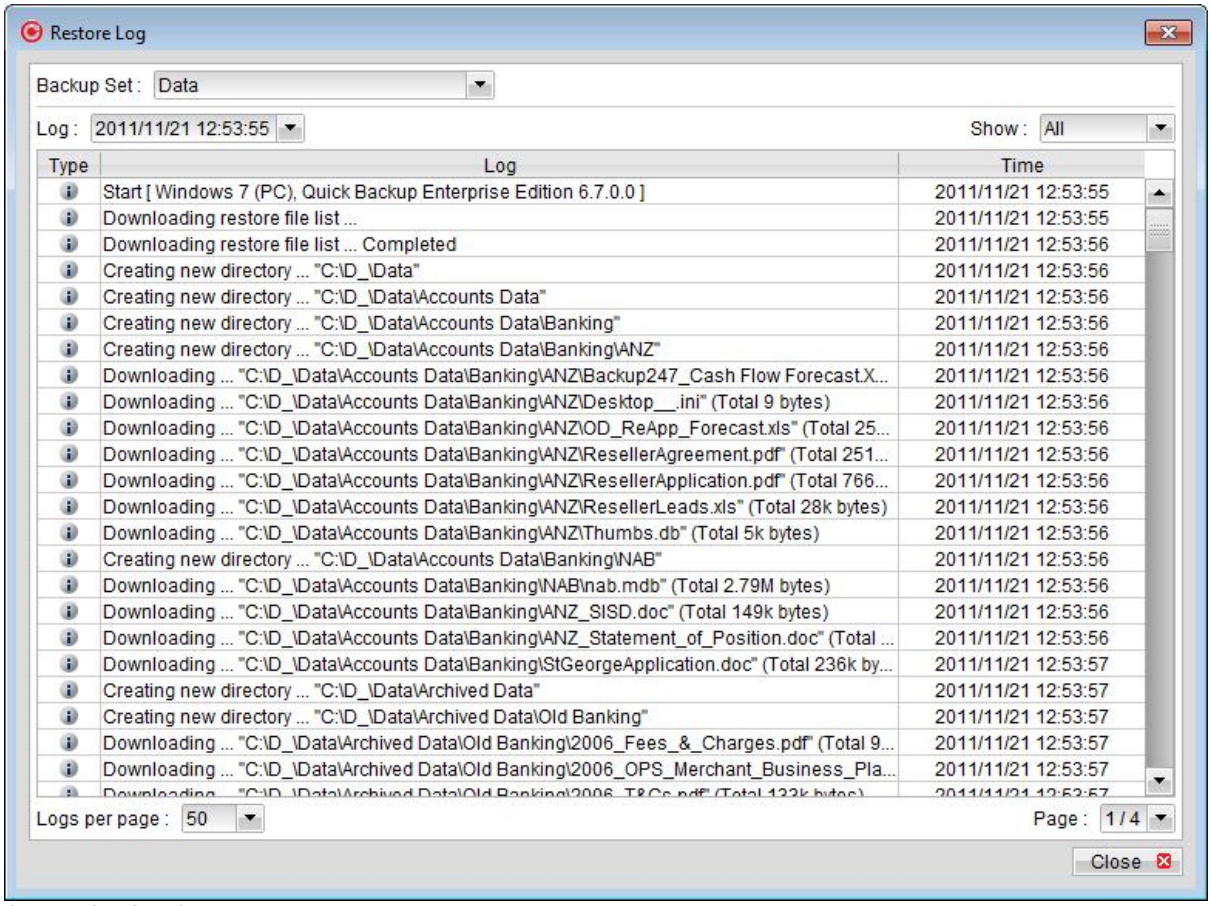

Backup Log
Backup Set : Data
Log : 2011/10/19 10:20:29
Show : All
Type
Log
Time
Start [Windows 7 (PC), Quick Backup Enterprise Edition 6.7.0.0] 2011/10/19 10:20:29
Using Temporary Directory C:\Users\Joe\temp 2011/10/19 10:20:29
Start running pre-commands 2011/10/19 10:20:29
Finished running pre-commands 2011/10/19 10:20:30
Start creating Shadow Copy Set ... 2011/10/19 10:20:30
Shadow Copy Set successfully created 2011/10/19 10:20:34
Downloading server file list ... 2011/10/19 10:20:35
Downloading server file list ... Completed 2011/10/19 10:20:37
Reading backup source from hard disk ... 2011/10/19 10:20:37
Uploading New Directory ... D:\Data\Client Documents 2011/10/19 10:20:38
Uploading New Directory ... D:\Data\Accounts Data 2011/10/19 10:20:38
Uploading New Directory ... D:\Data\Company Registartion 2011/10/19 10:20:38
Uploading New Directory ... D:\Data\Archived Data 2011/10/19 10:20:38
Uploading New Directory ... D:\Data\Contracts 2011/10/19 10:20:38
Uploading New Directory ... D:\Data\Invoices 2011/10/19 10:20:38
Uploading New Directory ... D:\Data\Databases 2011/10/19 10:20:38
Uploading New Directory ... D:\Data\Compliance 2011/10/19 10:20:38
Reading backup source from hard disk ... Completed 2011/10/19 10:20:39
Uploading New Directory ... D:\Data\Legal 2011/10/19 10:20:39
Uploading New Directory ... D:\ 2011/10/19 10:20:39
Uploading New Directory ... D:\Data 2011/10/19 10:20:39
Uploading New Directory ... D:\Data\Logos & Graphics 2011/10/19 10:20:39
Uploading New Directory ... D:\Data\Project Data 2011/10/19 10:20:39
Logs per page : 1000
Page : 1 / 1
Close
(Sample backup data)

Menu Item	Description
Backup Set	**Drop down menu for selecting which backup set.**
Log	**Drop down menu for selecting which log to review (in YYYY/MM/DD hh:mm:ss format).**
Show	**Drop down menu to filter display of only Information, Warning, Error, or all log entries.**
Logs per page	**Drop down menu for selecting the number of log entries to display per page.**
Page	**Drop down menu to switch the page number.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

5.7 Restore Log

Similar to backup, all restore activities are also logged to a corresponding log files. To review them, click on the [Restore Log] button.


Restore Log
Backup Set : Data
Log : 2011/11/21 12:53:55
Show : All
Type
Log
Time
Start [Windows 7 (PC), Quick Backup Enterprise Edition 6.7.0.0] 2011/11/21 12:53:55
Downloading restore file list ... 2011/11/21 12:53:55
Downloading restore file list ... Completed 2011/11/21 12:53:56
Creating new directory ... "C:\D_\Data" 2011/11/21 12:53:56
Creating new directory ... "C:\D_\Data\Accounts Data" 2011/11/21 12:53:56
Creating new directory ... "C:\D_\Data\Accounts Data\Banking" 2011/11/21 12:53:56
Creating new directory ... "C:\D_\Data\Accounts Data\Banking\ANZ" 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ\Backup247_Cash Flow Forecast.X... 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ\Desktop__.ini" (Total 9 bytes) 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ\OD_ReApp_Forecast.xls" (Total 25... 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ\ResellerAgreement.pdf" (Total 251... 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ\ResellerApplication.pdf" (Total 766... 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ\ResellerLeads.xls" (Total 28k bytes) 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ\Thumbs.db" (Total 5k bytes) 2011/11/21 12:53:56
Creating new directory ... "C:\D_\Data\Accounts Data\Banking\NAB" 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\NAB\nab.mdb" (Total 2.79M bytes) 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ_SISD.doc" (Total 149k bytes) 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ_Statement_of_Position.doc" (Total ... 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\StGeorgeApplication.doc" (Total 236k by... 2011/11/21 12:53:57
Creating new directory ... "C:\D_\Data\Archived Data" 2011/11/21 12:53:57
Creating new directory ... "C:\D_\Data\Archived Data\Old Banking" 2011/11/21 12:53:57
Downloading ... "C:\D_\Data\Archived Data\Old Banking\2006_Fees_&_Charges.pdf" (Total 9... 2011/11/21 12:53:57
Downloading ... "C:\D_\Data\Archived Data\Old Banking\2006_OPS_Merchant_Business_Pla... 2011/11/21 12:53:57
Logs per page : 50
Page : 1 / 4
Close
(Sample data)

Menu Item	Description
Backup Set	**Drop down menu for selecting which backup set.**
Log	**Drop down menu for selecting which log to review (in YYYY/MM/DD hh:mm:ss format).**
Show	**Drop down menu to filter display of only Information, Warning, Error, or all log entries.**
Logs per page	**Drop down menu for selecting the number of log entries to display per page.**
Page	**Drop down menu to switch the page number.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

6 Configure Backup Sets

This chapter describes how to configure a backup set.

A backup set defines the configuration of a backup routine, such as backup schedule, backup source and encryption setting as well as other options.

6.1 Backup Setting

Click on the [Backup Setting] button to:

- Create new backup set –

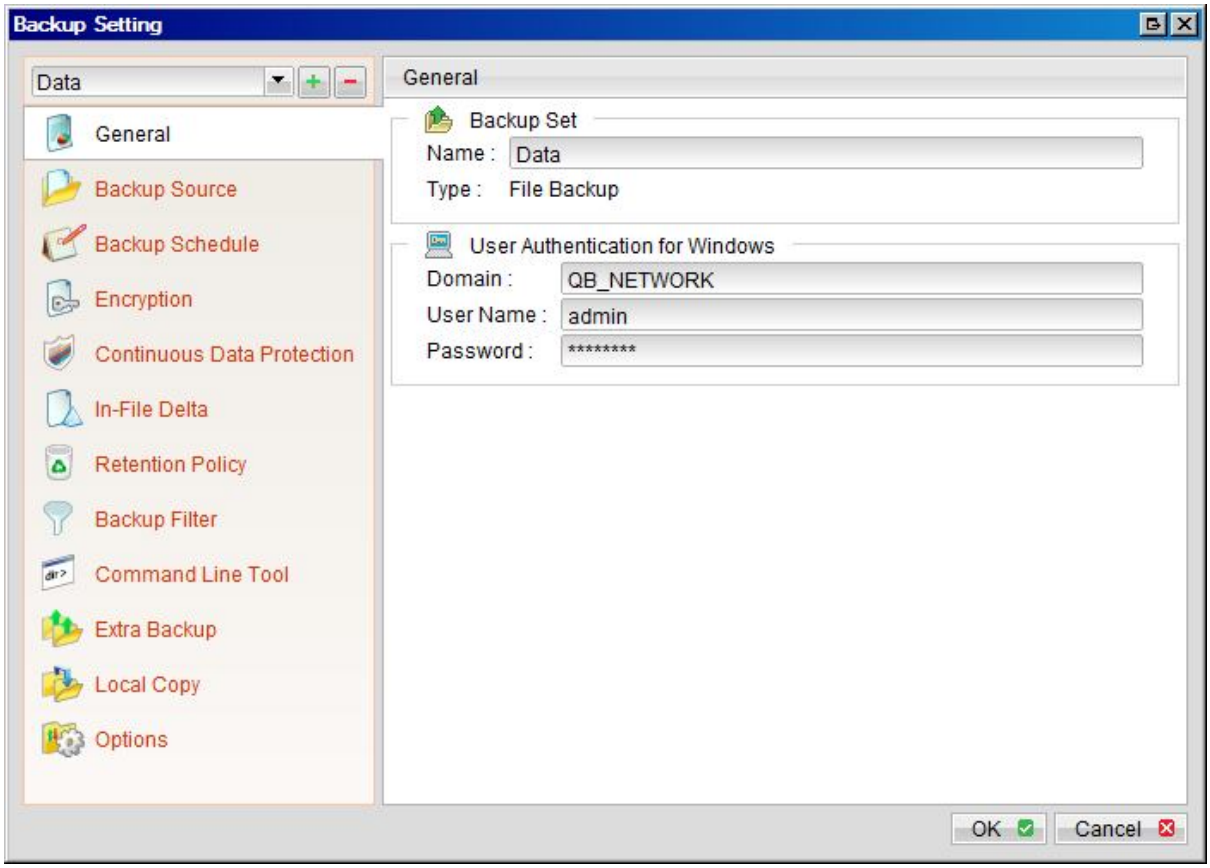
  Select the button to add a new backup set.

- Delete existing backup set –

  Select a backup set from the drop down menu, and the button to remove corresponding backup set.

- Modify existing backup set –

  Select a backup set from the drop down menu, and other options from the left panel to modify the backup set.



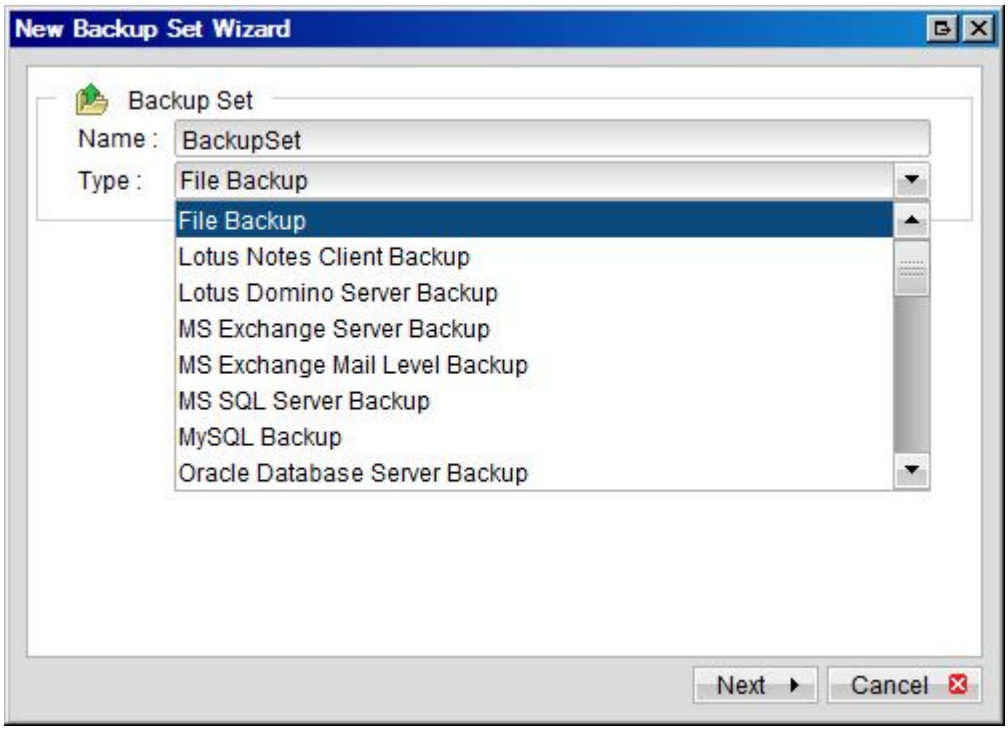
Icon	Menu Item	Description
	General	**Click to access the general backup set menu.**
	Backup Source	**Click to access the backup source selection menu.**
	Backup Schedule	**Click to access the backup schedule setting menu.**
	Encryption	**Click to access the encryption setting menu.**
	Continuous Data Protection	**Click to access the continuous data protection menu.**
	In-File Delta	**Click to access the In-file delta menu.**
	Retention Policy	**Click to access the retention policy menu.**
	Backup Filter	**Click to access the backup filter menu.**
	Command Line Tool	**Click to access the pre post command line tool menu.**

	Extra Backup	**Click to access the extra backup setting menu.**
	Local Copy	**Click to access the local copy backup menu.**
	Options	**Click to access the option menu.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

6.1.1 New Backup Set Wizard

Select the button to start the New Backup Set Wizard.



Select the corresponding backup type, in this case, a file backup set.

A backup set can be one of the following types:

Backup Type	Description
File	**Backup set type for backup of normal files.**
Lotus Domino Server	**Backup set type for backup of Lotus Domino server.**
Lotus Notes Client	**Backup set type for backup of Lotus Notes client.**

MS Exchange Server	**Backup set type for backup of Microsoft Exchange server.**
MS Exchange Mail Level	**Backup set type for backup of individual emails (brick level backup).**
MS SQL Server	**Backup set type for backup of Microsoft SQL server.**
MySQL Server	**Backup set type for backup of backup MySQL server.**
Oracle Database Server	**Backup set type for backup of Oracle database server**
System State	**Backup set type for backup of Microsoft Window's System State.**
ShadowProtect System	**Backup set type for Bare-Metal backup of your system using StorageCraft's ShadowProtect.**
Windows System	**Backup set type for Bare-Metal backup of your system using Microsoft's WBAdmin.**
MS VM	**Backup set type for backup of Virtual Machine on Microsoft Hyper-V server.**
VMware VM	**Backup set type for backup of Virtual Machine on VMware server (VM Server, ESX, ESXi).**

*The availability of backup type listed above may be service provider dependent. If a backup type is not available, please check with your service provider for further details and availability.

For exact application support list, please contact your service provider for further details.

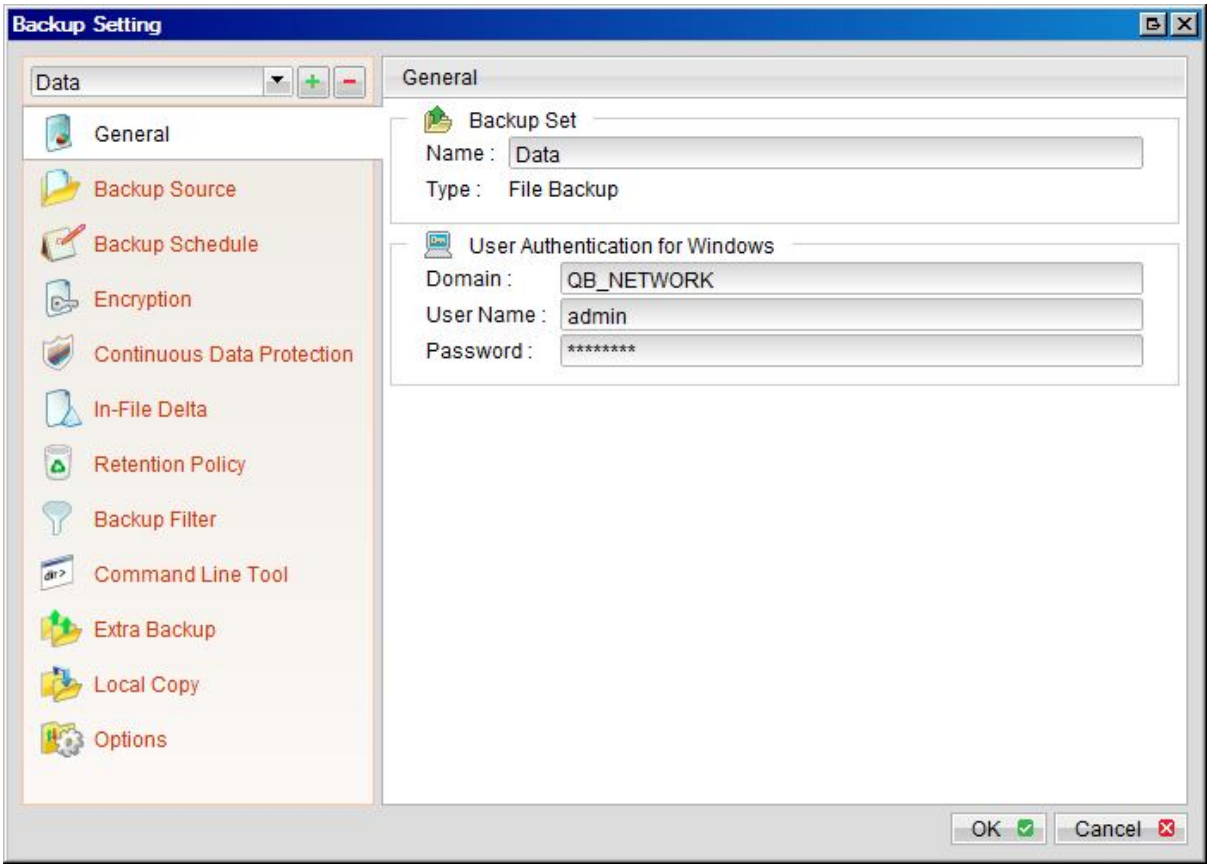
Note: Backup set type is defined at the backup set creation time, and **cannot be modified afterward**.

Next few steps of a new backup set creation process, including Backup Source, Backup Schedule and Encryption setting configuration are discussed in the following sections of the guide.

6.1.2 General

Click on the [General] tab to modify the [User Authentication for Windows] setting.

For backup of network shared drive, you need to specify a Windows domain account for the backup client application with sufficient permission to access the network location (by default, the backup application services run as Local System, which does not have permission for accessing network resource).



Menu Items	Description
Domain	**Input box for entering domain of the Windows domain account.**
User Name	**Input box for entering username of the Windows domain account.**
Password	**Input box for entering password of the Windows domain account.**

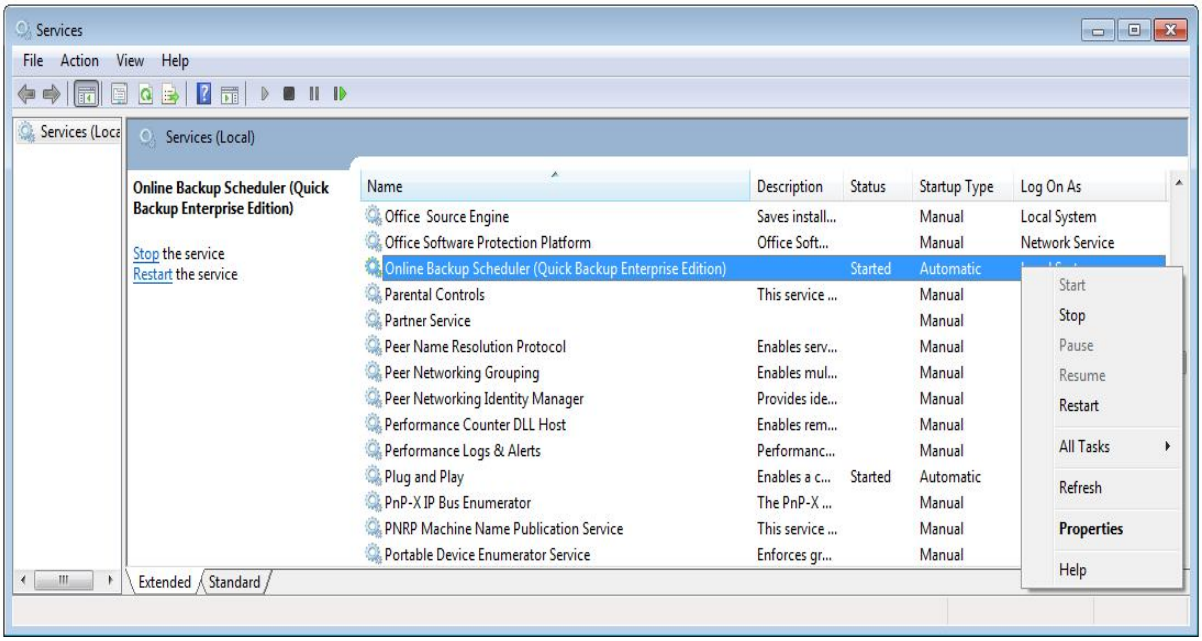
*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Enter the login credentials of a Windows domain account with sufficient permission to access the network shared drive to allow access for Quick Backup.

Please also modify the Log On account of the backup application's scheduler service.

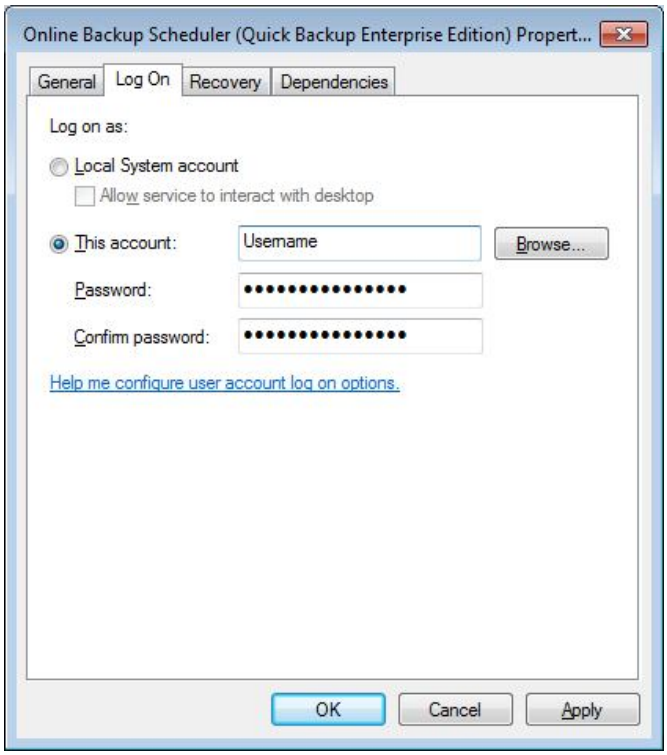
1. Under [Control Panel], select [Administrative Tools] and [Services].

2. Right click on [Online Backup Scheduler (Quick Backup Enterprise Edition)].



3. Select [Properties], and the [Log On] tab.

4. Select [This account], and enter the login credentials of a Windows domain account with sufficient permission to access the network shared drive.



5. This will allow the backup application to access the network shared drive for backup.

Note: The steps above assumed that the corresponding network location is already mapped on the operating system level.

6.1.3 Backup Source

Click on the [Backup Source] tab to configure backup source of a backup set.

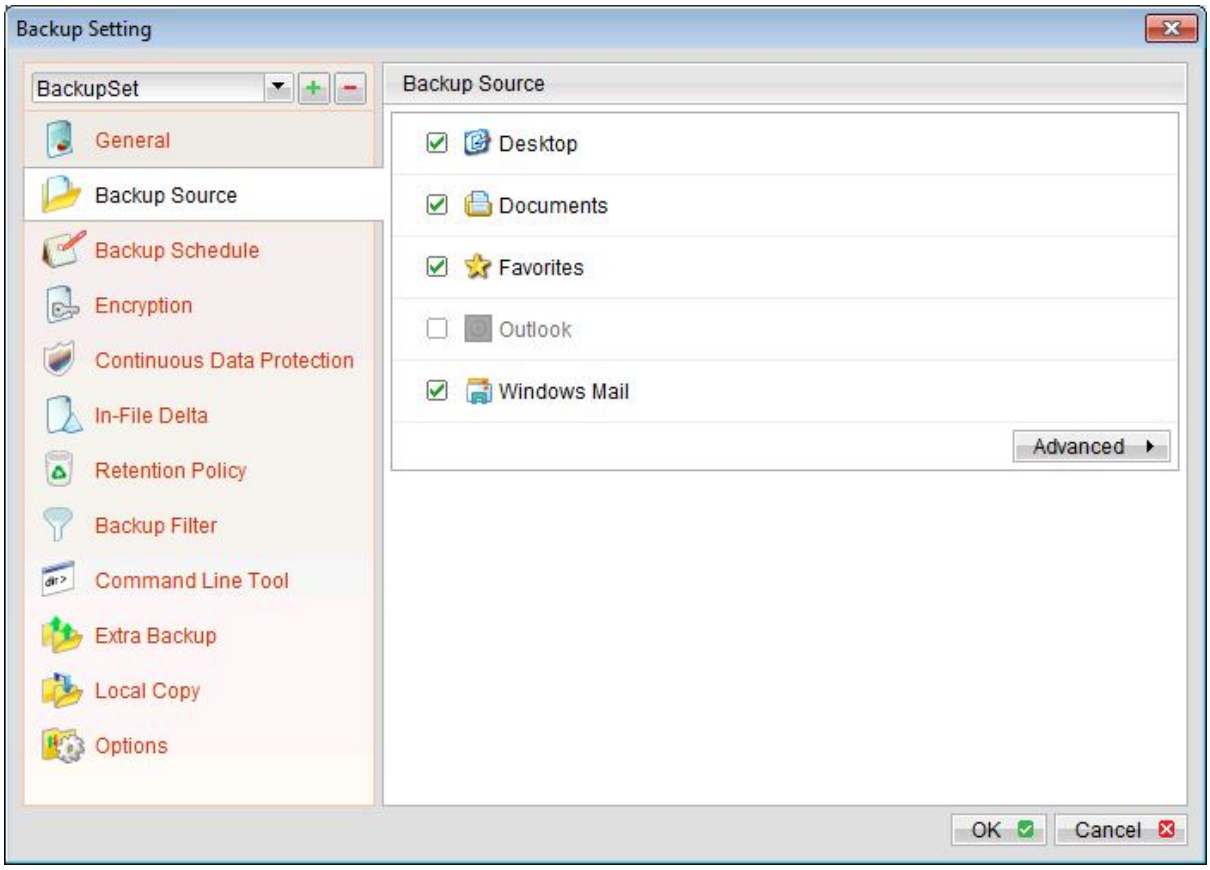
A Backup Source defines the files and directories to be included for backup.

There are two types of backup source: Selected and Deselected.

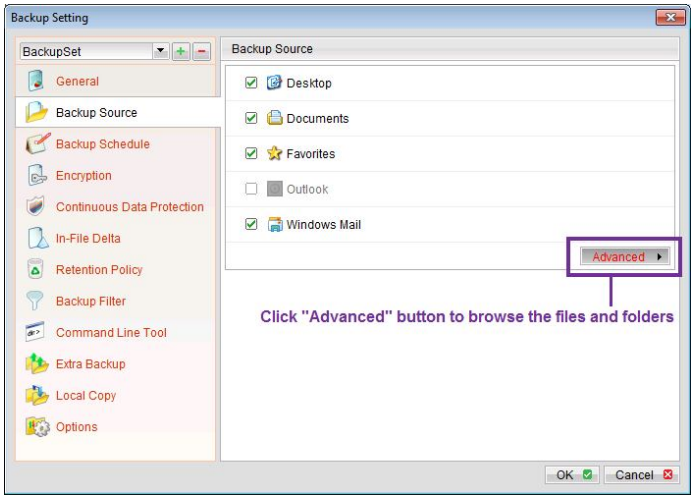
- Selected backup source defines files and directories that are to be included in a backup set.
- Deselected backup source defines files and directories that are to be excluded from a backup set.

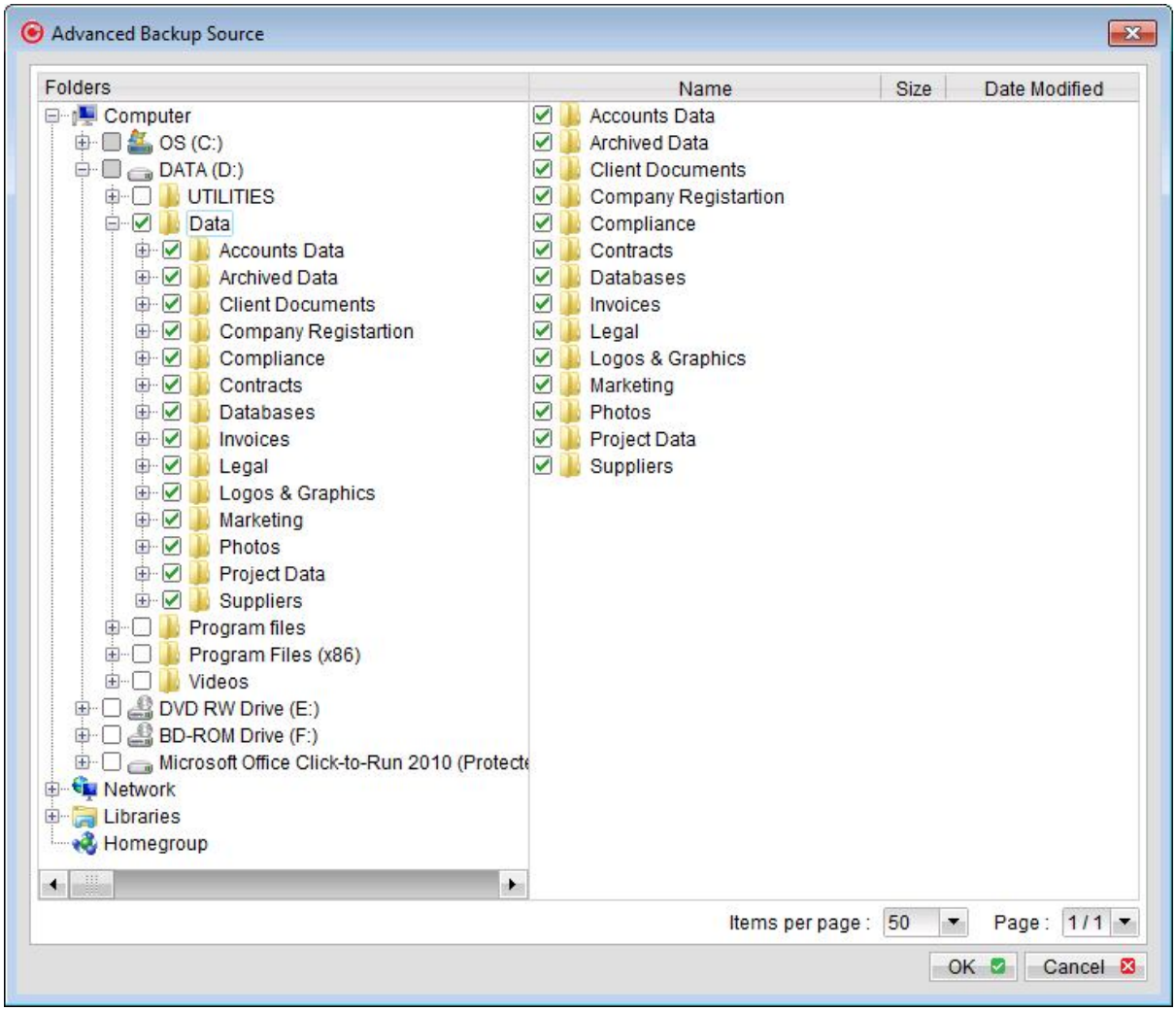
On the basic backup source selection dialog, you can select directories that are commonly selected as backup source for backup:

- Desktop folder
- My Documents folder
- Favorites folder
- Outlook and Outlook Express folder



Click on [Advanced] button to access the advanced backup source dialog to select other directories for backup.





The checkbox beside a root drives, directory or file can be in one of the following mode:

Mode	Description
☑	**All directories and files under this directory will be backed up.**
☑	**All directories and files under this directory except those explicitly excluded will be backed up.**

	Directories and files selected to this directory in the future will be backed up as well.
☐	**Only the checked directories and files under this directory will be backed up.** **Directories and files selected to this directory in the future will not be backed up.**
☐	**No directory or file under this directory will be backed up.**

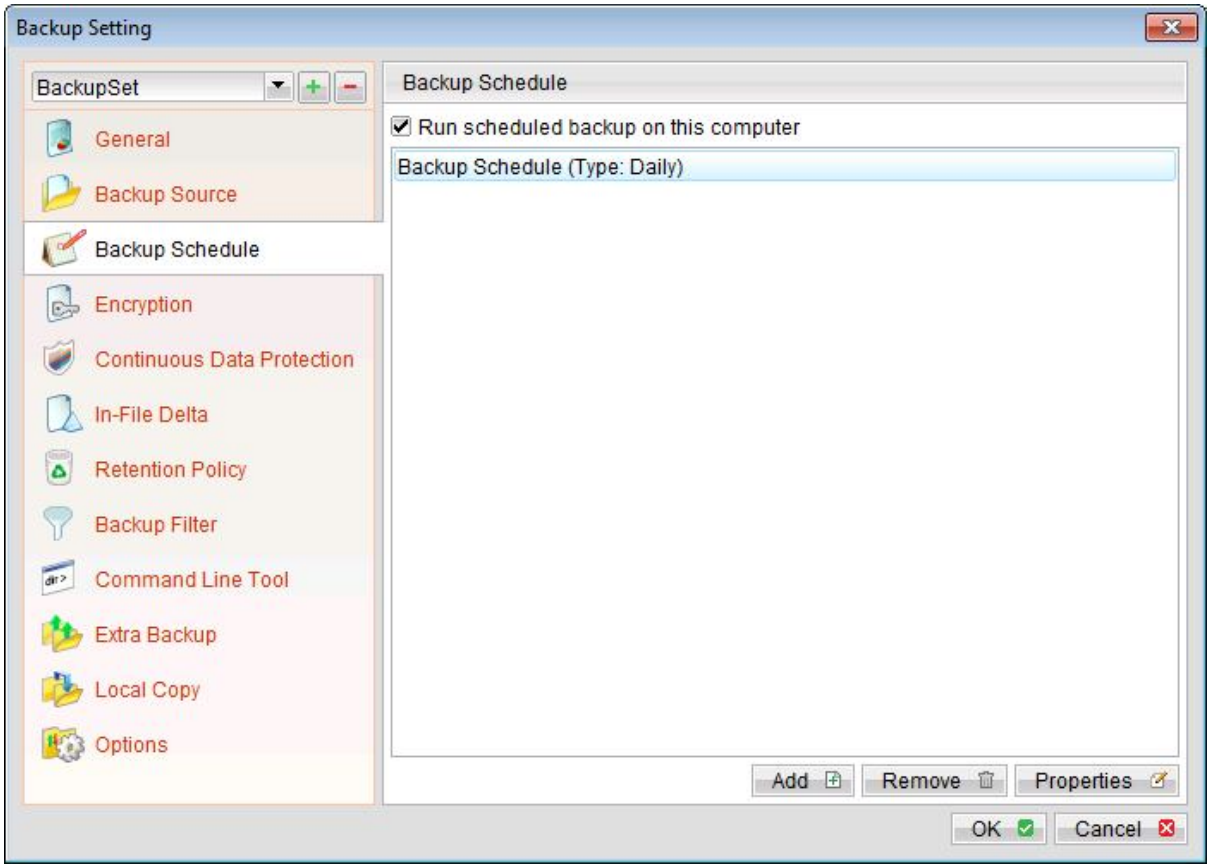
Note: For installation on Windows platforms, hidden directories and files will be displayed only if the [Hide protected operating files] setting of Windows Explorer is disabled.
By selecting a parent directory as backup source, all child directories and files including any hidden directories or files would be backup as well.

To avoid backing up hidden directories such as the Recycle Bin folder, please select the corresponding directories or files required as backup source directly, instead of selecting the parent directory or root drive letter.

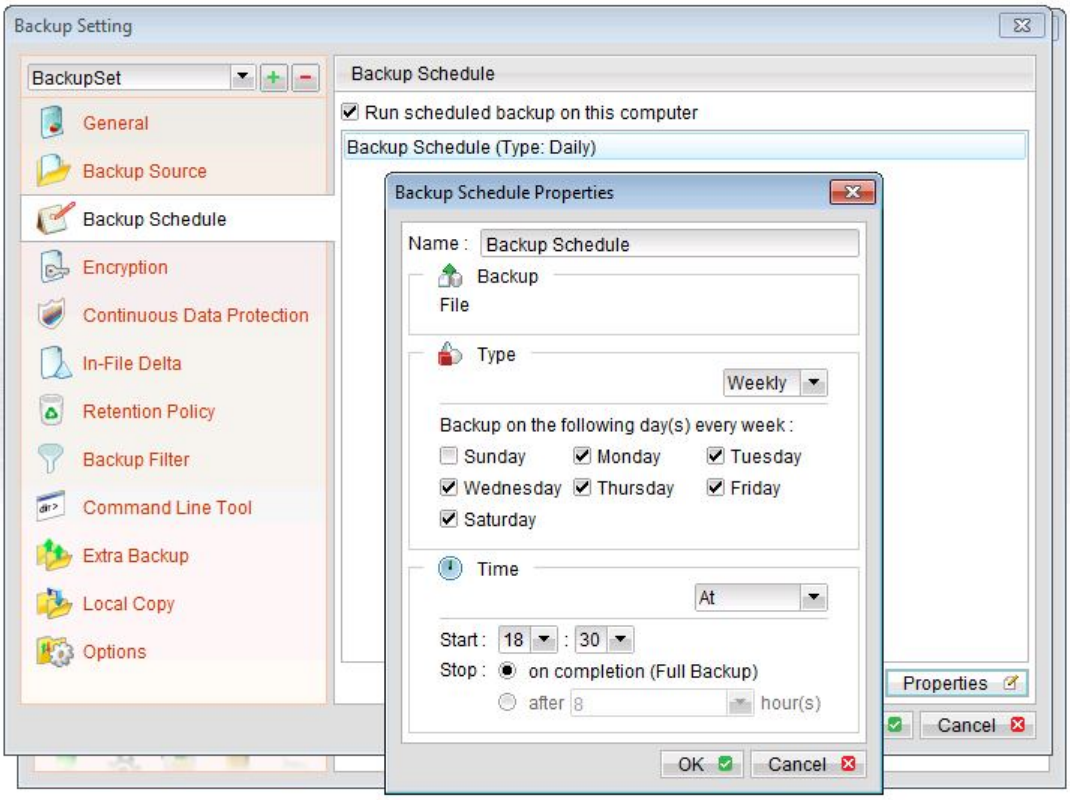
6.1.4 Backup Schedule

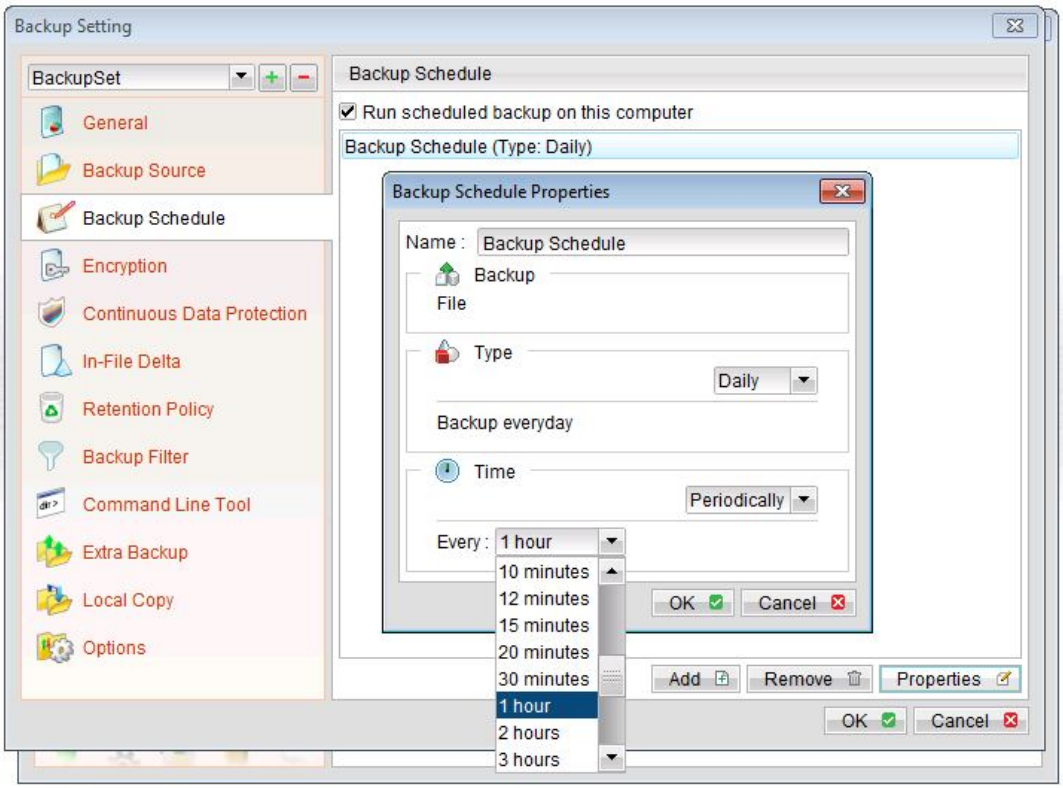
Click on the [Backup Schedule] tab of the backup setting menu to configure backup schedule of a backup set.

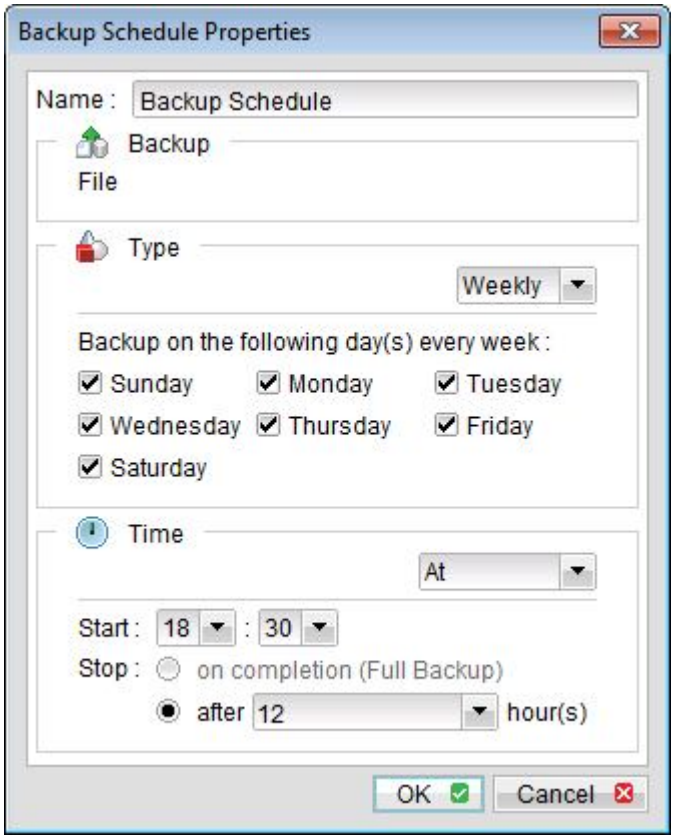
A Backup Schedule defines the time, time period allowed, and frequency that backup job for an existing backup set should be run automatically.



Menu Items	Description
Run scheduled backup on this computer	**Checkbox to enable or disable the corresponding backup set to run on this computer.**
Add	**Click to add a new backup schedule.**
Remove	**Click to remove an existing backup schedule.**
Properties	**Click to modify an existing backup schedule.**


Backup Setting
BackupSet
General
Backup Source
Backup Schedule
Encryption
Continuous Data Protection
In-File Delta
Retention Policy
Backup Filter
Command Line Tool
Extra Backup
Local Copy
Options
Backup Schedule
Run scheduled backup on this computer
Backup Schedule (Type: Daily)
Backup Schedule Properties
Name : Backup Schedule
Backup
File
Type
Weekly
Backup on the following day(s) every week :
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Time
At
Start : 18 : 30
Stop : on completion (Full Backup)
after 8 hour(s)
OK
Cancel
Properties
Cancel


Backup Setting
BackupSet
General
Backup Source
Backup Schedule
Encryption
Continuous Data Protection
In-File Delta
Retention Policy
Backup Filter
Command Line Tool
Extra Backup
Local Copy
Options
Backup Schedule
Run scheduled backup on this computer
Backup Schedule (Type: Daily)
Backup Schedule Properties
Name : Backup Schedule
Backup
File
Type
Daily
Backup everyday
Time
Periodically
Every : 1 hour
10 minutes
12 minutes
15 minutes
20 minutes
30 minutes
1 hour
2 hours
3 hours
OK
Cancel
Add
Remove
Properties
OK
Cancel



Menu Items	Description
Name	**Input box for entering backup schedule name.**
Type	**Checkbox to select schedule type.** **Daily - Backup job will run everyday at a specific time under this schedule type** **Weekly - Backup job will run on specific day(s) of a week, at a specific time under this schedule type.** **Monthly - Backup job will run on specific day of a month (date, or special criteria such as first weekend, last weekday), at a specific time under this schedule type.** **Custom - Backup job will run on specific day of a year (date), at a specific time under this schedule type.**
Time (At)	**To start backup job at a specific time.** **Start - Dropdown menu to select the start time of a backup job.** **Stop – Option to allow a backup job to run to completion, or to stop the running backup job after a specified hour.**

Time (Periodically)	**To start backup job at regular intervals of time.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

To configure a **Daily** backup schedule where backup job will run everyday at 8:00pm:

1. Select [Add] to open the [Add new backup schedule] dialog.
2. Enter name of the backup schedule.
3. Select [Daily] from the schedule [Type] dropdown menu.
4. Select [At] from the [Time] dropdown menu.
5. Configure start time to be 20:00
6. Configure the stop option according to your requirement.

To configure a **Weekly** backup schedule where backup job will run on Friday every week at 8:00pm:

1. Select [Add] to open the [Add new backup schedule] dialog.
2. Enter name of the backup schedule.
3. Select [Weekly] from the schedule [Type] dropdown menu.
4. Select the checkbox beside [Friday].
5. Select [At] from the [Time] dropdown menu.
6. Configure start time to be 20:00
7. Configure the stop option according to your requirement.

To configure a **Monthly** backup schedule where backup job will run on first weekend of every month at 8:00pm:

1. Select [Add] to open the [Add new backup schedule] dialog.
2. Enter name of the backup schedule.
3. Select [Monthly] from the schedule [Type] dropdown menu.
4. Select [First], [Weekend].
5. Select [At] from the [Time] dropdown menu.
6. Configure start time to be 20:00
7. Configure the stop option according to your requirement.

To configure a **Custom** backup schedule where backup job will run on Jan 1st of 2012 (2012-01-01) at 8:00pm:

1. Select [Add] to open the [Add new backup schedule] dialog.
2. Enter name of the backup schedule.
3. Select [Custom] from the schedule [Type] dropdown menu.
4. Enter the date when the backup should be performed (YYYY-MM-DD).
5. Configure start time to be 20:00
6. Configure the stop option according to your requirement.

Note that multiple backup schedules of different type (e.g. daily, weekly) can be configured for a single backup set.

For example:

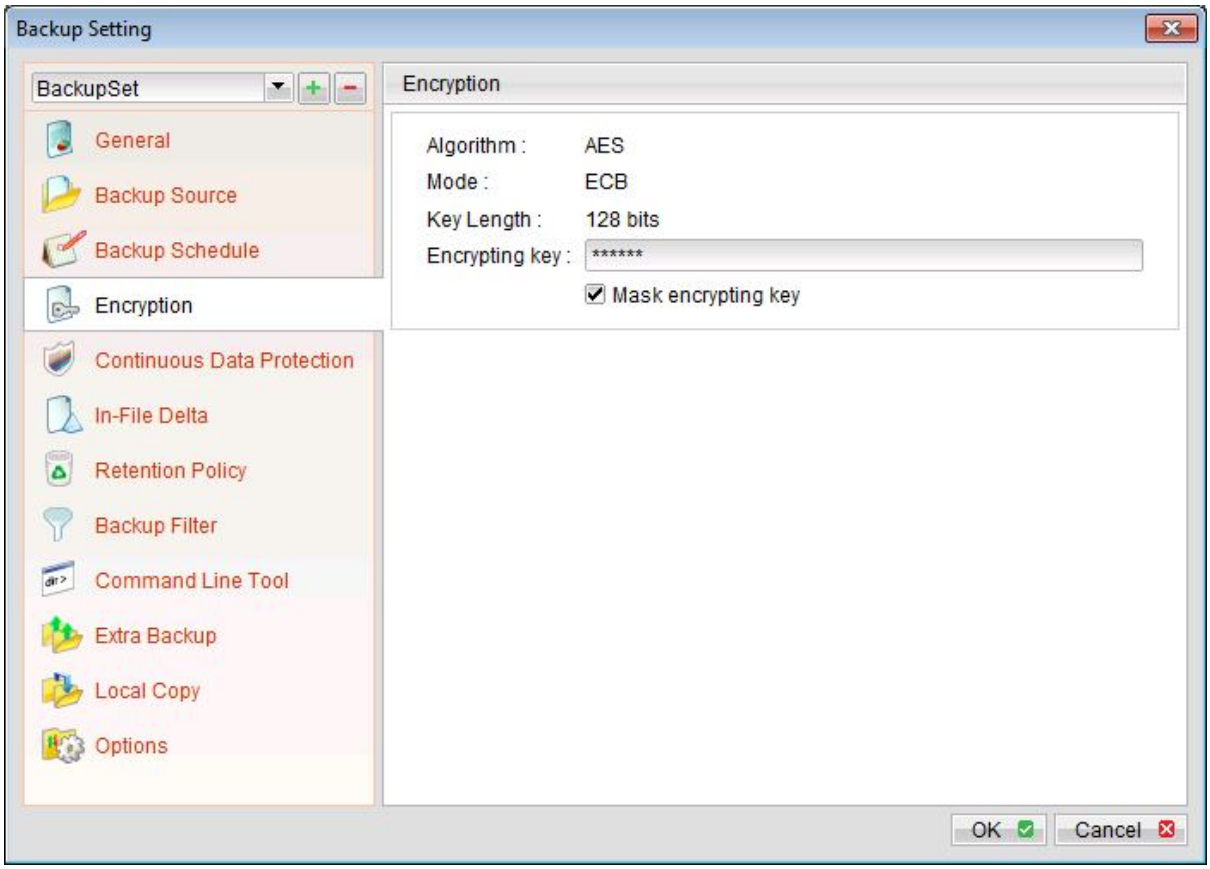
- Daily backup schedule at 00:00
- Daily backup schedule at 12:00
- Weekly backup schedule on Friday at 18:00

Combination of these schedules effectively creates a schedule for backup at 00:00 and 13:00 everyday, and 18:00 every Friday.

6.1.5 Encryption

Before files are uploaded to the backup server, they are first compressed and encrypted with an algorithm, mode and key of your choice.

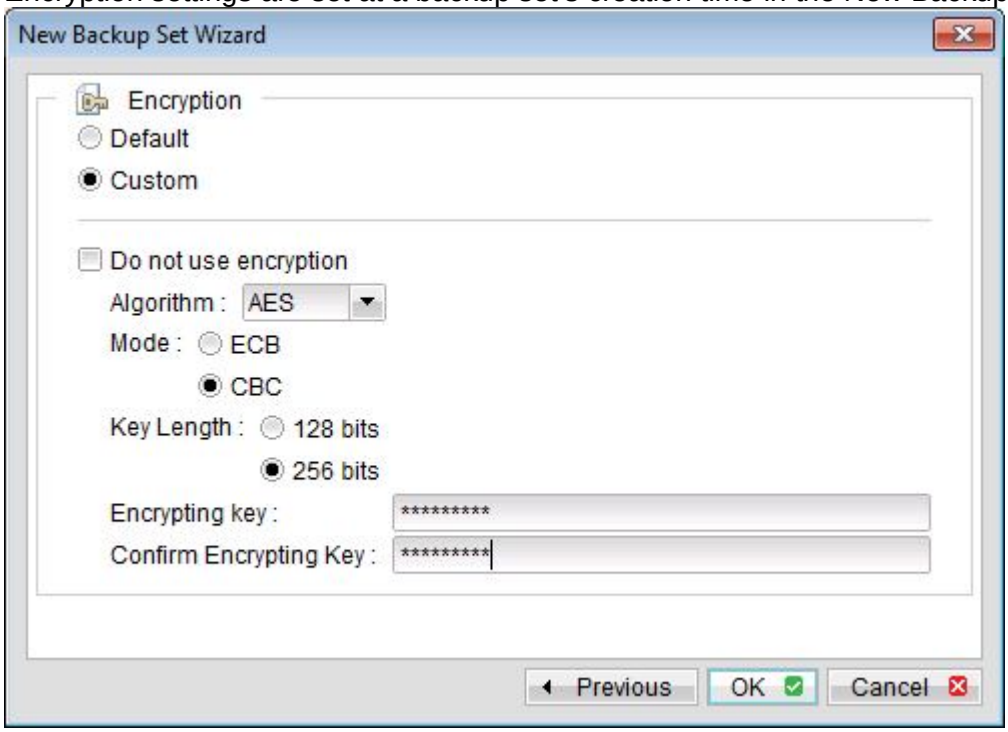
Select the [Encryption] tab to view the current encryption setting of an existing backup set.



Menu Items	Description
Encryption key	**Text box displaying the encryption key for the corresponding backup set.**
Mask encryption key	**Checkbox to enable or disable masking of the encrypting key.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Encryption settings are set at a backup set's creation time in the New Backup Set Wizard.



Menu Items	Description
Default	**Radio button to select default encrypting key.** **Default encryption setting -** **Encryption algorithm: AES** **Encryption mode: ECB** **Key Length: 256 bits** **Encrypting key: Same as current password**
Custom	**Radio button to select your custom encryption setting, including:** **Encryption algorithm** **Encryption mode** **Key Length** **Encrypting key**
Do not use encryption	**Checkbox to disable encryption (not recommended).**
Algorithm (used with Custom)	**Dropdown menu to select the encryption algorithm setting:** **Twofish - Twofish algorithm** **DESede - Triple DES algorithm** **AES - Advanced Encryption Standard algorithm**
Mode (used with Custom)	**Radio button to select ECB or CBC encryption**

	mode: **ECB - Electronic Cook Book mode** **CBC - Cipher Block Chaining mode**
Key Length (used with Custom)	**Radio button to select 128 bit or 256 bit key length.**
Encrypting key (used with Custom)	**Input box for entering your choice of encrypting key.**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Select [Default] encryption setting if you are not familiar with encryption algorithm or mode. The default encryption setting is:

Encryption algorithm: AES
Encryption mode: ECB
Key Length: 256 bits
Encrypting key: Same as current password

Encryption settings are set at a backup set's creation time and cannot be modified afterward.

If you are entering your own encrypting key, please considering selecting an encryption key with more than 8 characters, containing at least two of the following three character groups:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Numerals (0 through 9)

Important: By selecting default encryption setting, password string of the backup account will be configured as encrypting key (for the corresponding backup set).

The encryption key is independent from a backup account's password.

Since encryption settings are set at a backup set's creation time, even if the password is changed afterward, the encryption key remain the same.

It is VERY IMPORTANT that the encryption key is written down, and additional copies of the key are made, and stored in safe places so that it is readily available when needed to restore data.

If you lose the encryption key, the data is irretrievable.

For initial login of **existing backup user on new computer**, you will be prompted for the encrypting key of all existing backup set.

Menu Item	Description

Enter Correct Encrypting Key	**Input box for entering encrypting key of existing backup set.**
OK	**Click to confirm on encrypting key.**
Cancel	**Click to proceed without using encrypting key.**

Enter the correct encrypting key and click [OK] to proceed.

Alternatively, if the encrypting key is lost, press [Cancel] to proceed without encryption (e.g. for all backup job performed afterward).

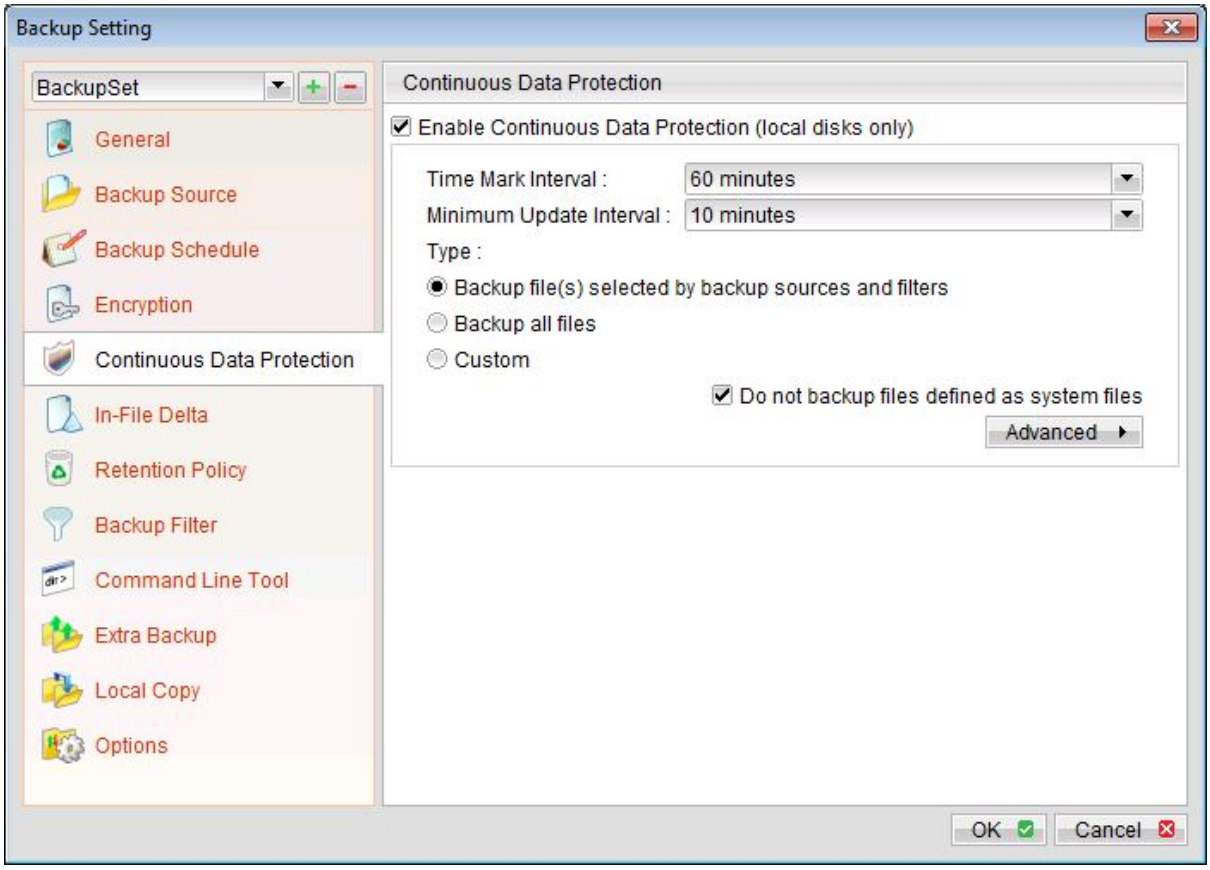
This would allow data backed up in the future to be restore-able (as they are no longer encrypted), but existing data that are already encrypted by the lost encrypting key would not be restore-able.

In case of lost encrypting key, it is strongly recommended that a new backup set be created, to ensure that data backed up in the future is encrypted and restore-able.

6.1.6 Continuous Data Protection (CDP)

Continuous Data Protection (CDP) is a feature providing backup for selective data whenever change is made. Depending on the option selected, every version of a file is backed up close to real time.

To enable CDP, click on the [Continuous Data Protection] tab and select the [Enable Continuous Data Protection] checkbox.



Menu Items	Description
Enable Continuous Data Protection	**Checkbox to enable or disable CDP.** **Note: CDP will only backup directories and files on local drive, but not on floppy drive, removable drive or network drive.**
Time Mark Interval	**Defines a regular interval of time (e.g. every x minutes), with each interval containing one snapshot (the first backup of each interval) available for restore.** **For example, for [Time Mark Interval] set**

	to 60 minutes, with the file updated every 5 minutes. A restore-able snapshot of the file will be available for each interval: **00:05, 01:05, 02:05, 03:05 ... etc.**
Minimum Update Interval	**Defines how often an updated file is backed up to the backup server.** **For example, for [Minimum Update Interval] set to [Always], file will be backed up to the server as they are updated.**
Backup file(s) selected by backup sources and filters	**Radio button to select if CDP will only backup modified directories or files selected as backup source.**
Backup all files	**Radio button to select if CDP will back up all modified directories and files on all local drive.**
Custom	**Radio button to select if CDP will backup a custom set of directories and files.** **Note: This custom set of directories and files can be different than the backup source selected for the backup set.**
Backup Source (used with Custom)	**Add – Click to select a custom set of directory or file as backup source for CDP backup.** **Remove – Click to remove a selected directory or file as backup source for CDP backup.** **Properties – Click to modify a selected directory or file as backup source for CDP backup.**
Backup Filter (used with Backup all files or Custom)	**Add – Click to create a backup filter for CDP backup.** **Remove – Click to remove a backup filter for CDP backup.** **Properties – Click to modify a backup filter for CDP backup.** **Note: Backup filter is case sensitive.**

Do not backup files defined as system files	**When this option is enabled, CDP will automatically exclude the following files from its backup:** **C:\hiberfil.sys** **C:\Pagefile.sys** **C:\Program Files*** **C:\RECYCLER** **C:\System Volume Information** **C:\Windows*** **${App_Data}\Avg7** **${App_Data}\Avg8** **${App_Data}\Kaspersky Lab** **${App_Data}\McAfee** **${App_Data}\McAfee.com** **${App_Data}\Microsoft** **${App_Data}\Sophos** **${App_Data}\Symantec** ****.tmp** ***\Application Data\Macromedia*** ***\Application Data\Mozilla*** ***\Local Settings\Application Data\Microsoft*** ***\ntuser.dat**
Advanced	**Click to access advanced CDP backup control to backup only when:** **CPU usage is less than a specific percentage.** **Network traffic is less than a specific Megabyte per second.** **No keyboard or mouse input exceeding a specific time (in minute).**

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Configure the [Time Mark Interval] and [Minimum Update Interval] according to your recovery requirement.

Time mark interval defines a regular interval of time, where each interval contains one snapshot available for restore.

For example, when [Time Mark Interval] is configured to 60 minutes. 24 intervals would be marked per day, with each interval spanning across 60 minutes:

Interval 1 – 00:00 to 01:00
Interval 2 – 01:00 to 02:00
Interval 3 – 02:00 to 03:00
Interval 4 – 03:00 to 04:00

To

Interval 23 – 22:00 to 23:00
Interval 24 – 23:00 to 24:00

Assuming that a file is backed up multiple times (by CDP) within each interval, the first backup (e.g. snapshot) of each interval would be available for restore.

Minimum update interval defines the minimum period of time before an updated file is backed up to the backup server.

For example, when [Minimum Update Interval] is configured to 10 minutes, updated file would be backed up to the backup server every 10 minutes. To ensure that updated files are always uploaded to the server immediately, you can consider setting the [Minimum Update Interval] as Always.

To configure CDP for backup of the **directories and files selected as backup source**:

1. Select the [Backup file(s) selected by backup sources and filters] radio button for [Type].

To configure CDP for backup of **all local drive(s)**:

1. Select the [Backup all files] radio button for [Type].
2. Configure [Backup Filter] for inclusion or exclusion of file if necessary.

To configure CDP for backup of a **custom set of directories or files**:

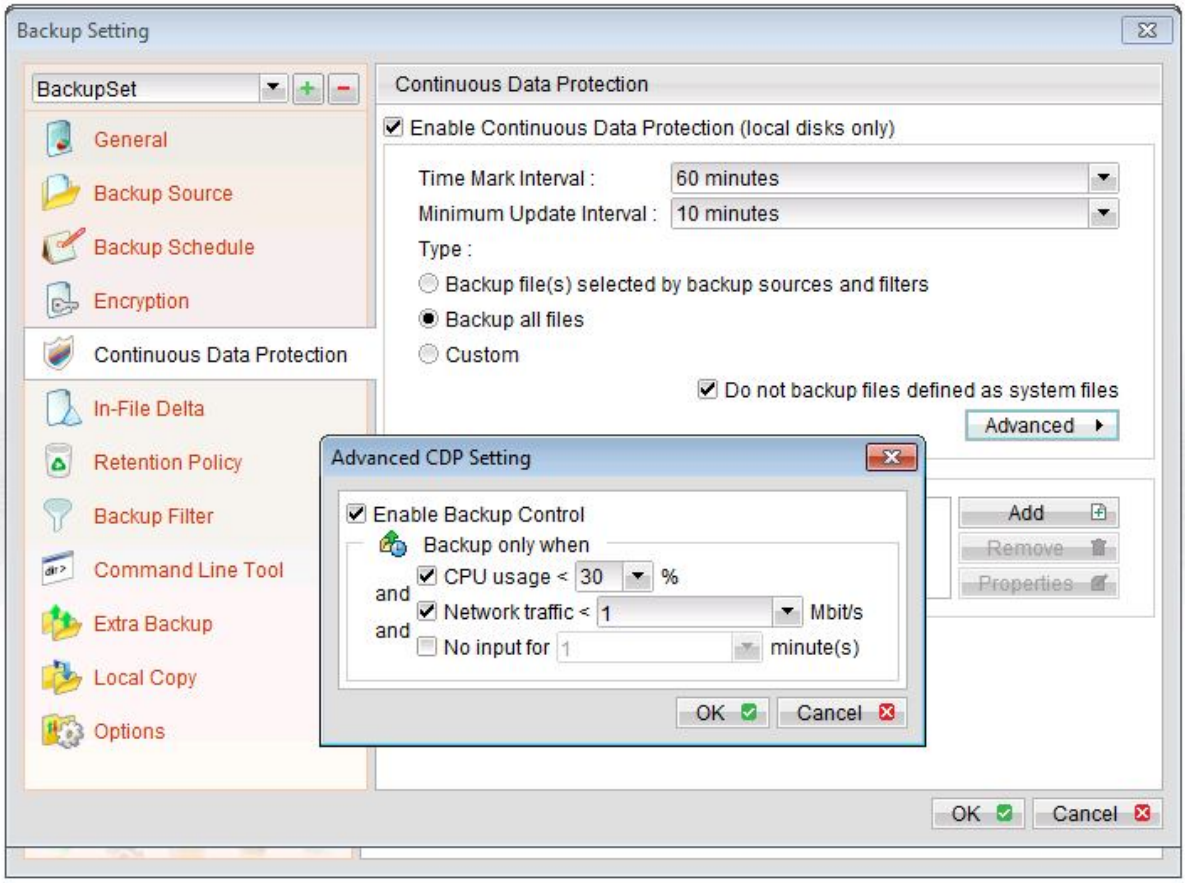
1. Select the [Custom] radio button for [Type].
2. Click [Add] beside the [Backup Source] section (within the CDP tab).
3. Select the custom set of data for backup.
4. Configure [Backup Filter] for inclusion or exclusion of file if necessary.

Note that the backup filter function is only available for CDP type [Backup all files] or [Custom].

Although CDP can be a helpful feature, the protection offered by CDP is often heralded without consideration of the disadvantages that it can present.

Specifically, the continuous CPU, memory and bandwidth usage can adversely affect the corresponding machine’s performance.

To enable backup control for CDP backup, select [Advanced] to open the advanced CDP setting dialog:



To allow CDP backup only when CPU usage is under 50%:

1. Select the checkbox beside [CDP usage].
2. Select the corresponding percentage from the [%] dropdown menu.

To allow CDP backup only when network traffic is under 10 Mbit/s:

1. Select the checkbox beside [Network traffic]
2. Enter the corresponding number in the [Mbit/s] textbox.

To allow CDP backup only when there is no keyboard or mouse input for 5 minutes:

1. Select the checkbox beside [No input for].
2. Enter the corresponding number (in minutes) in the [minute(s)

Important: Continuous Data Protection (CDP) will only backs up data selected as backup source after the CDP module is enabled. Existing data that are not updated will not be backed up by the CDP module.

Furthermore, CDP is not a replacement for the traditional schedule backup but works along with the scheduled backup to provide timely protection for your data.

CDP will automatically be stopped when a manual or scheduled backup is started, and will resume when the job is completed.

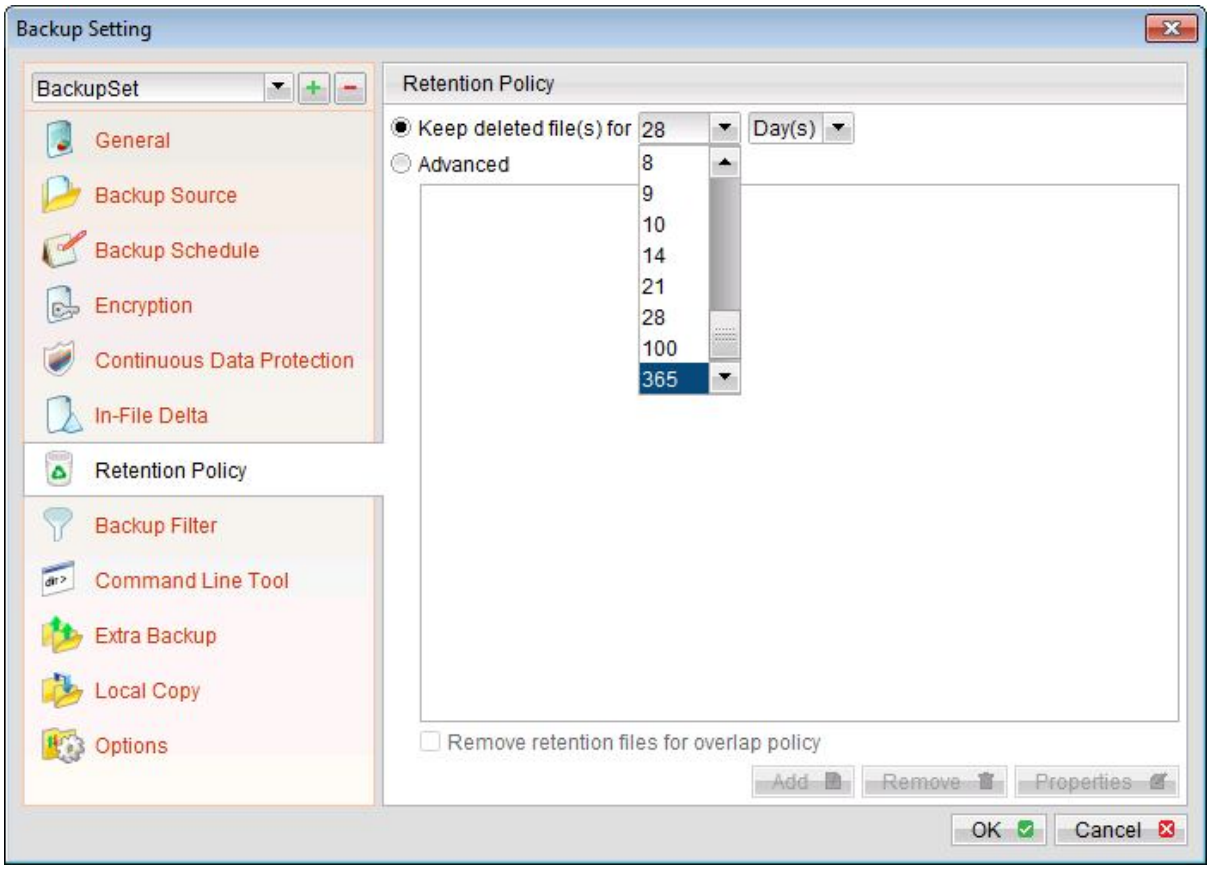
Note: It is not possible to run multiple CDP backup sets on the same machine with different backup user accounts.

6.1.7 In-File Delta

For more details about the In-file delta technology, please refer to the In-File Delta Technology section to be followed in this guide.

6.1.8 Retention Policy

Click on the [Retention Policy] tab to modify the retention policy of an existing backup set.



Retention policy defines the policies of persistent data management for meeting business data archival requirements.

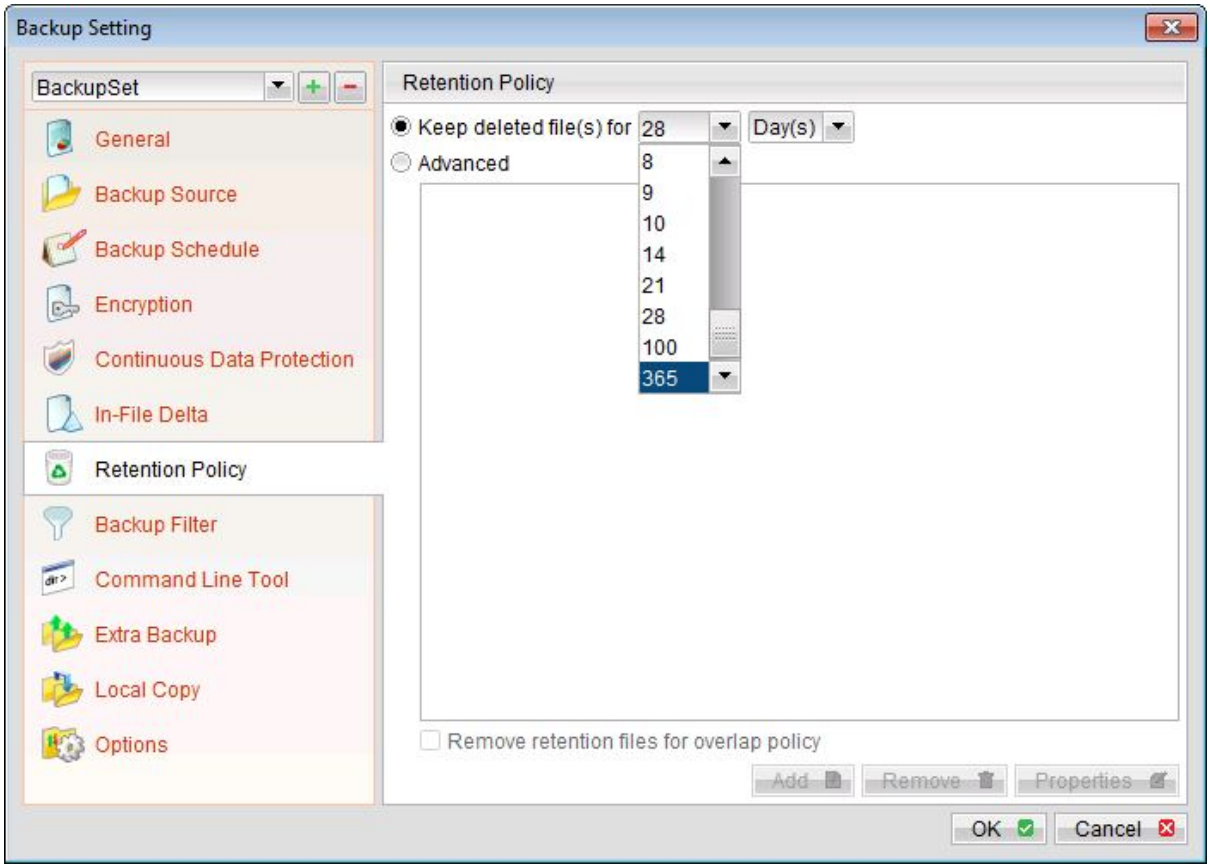
When a backup job is performed, for data that are modified or deleted on the client computer, their existing version on the backup server (backed up previously) would be moved into retention area, while newly backed up file would be placed in the current data area.

Specifically, retention policy setting defines how long are these data kept within the retention area before they are deleted permanently from the backup server.

For backed up data that have not been updated or deleted from the client computer, they are kept in the data area on the backup server and remain untouched.

A **standard retention policy** defines a basic policy where retained file (in the retention area) are removed automatically after a user specific number of days or backup jobs.

To define a standard retention policy, simply modify the [Keep delete file(s) for] drop down menu to your required days or jobs. Press [OK] and save before exiting the backup application to confirm the changes.



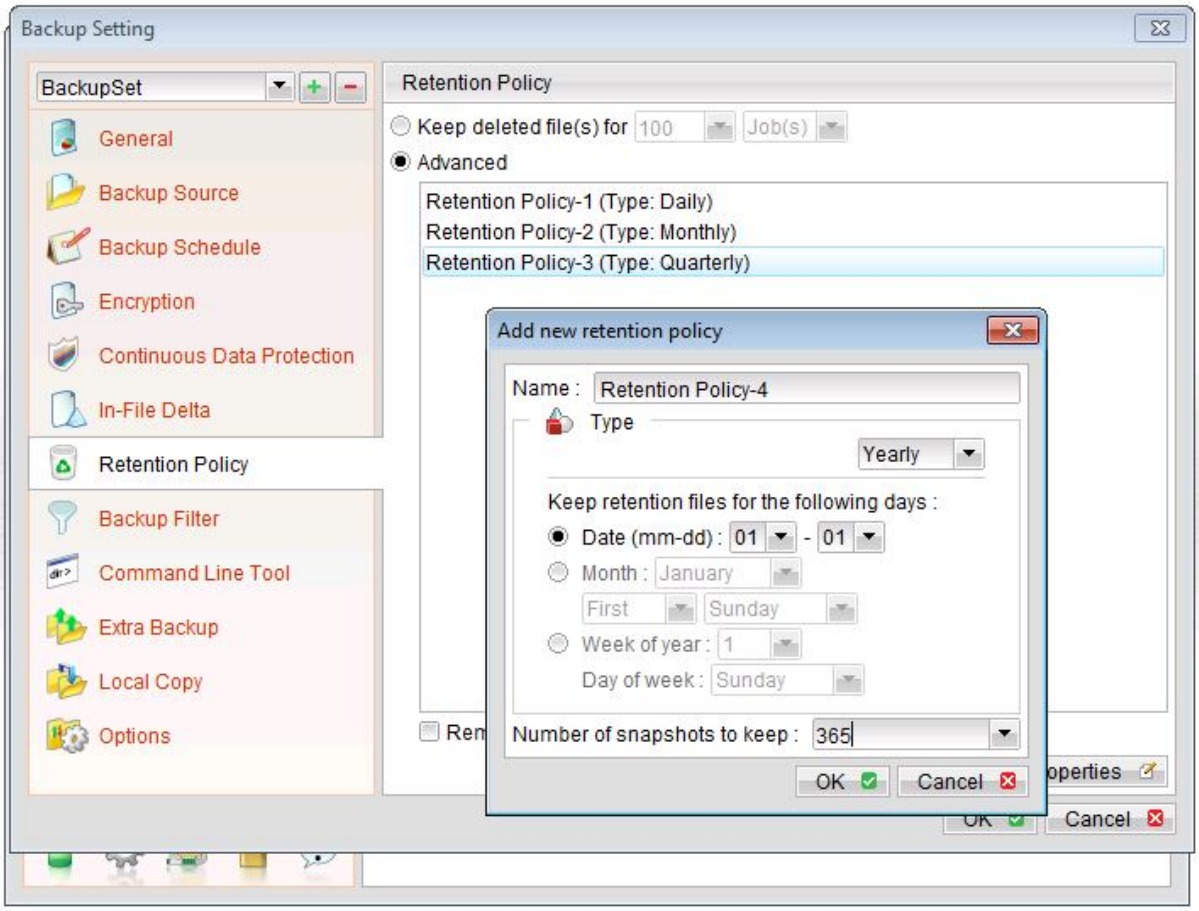
An **advanced retention policy** defines a more advanced and flexible policy where retained file (in the retention area) are removed automatically after a combination of user defined policy, such as:

- A specific number of days
- A specific number of weeks, including the day of the week
- A specific number of months, including the day of the month
- A specific number of years, including the day of the year

To define an advanced retention policy, select the [Advanced] button, and press the:

- [Add] button to add new policy
- [Remove] button to remove existing policy
- [Properties] to edit existing policy

Press [OK] and save before exiting the backup application to confirm the changes.



For example, you can configure the advanced retention policy to keep all data backed up:

- In the last 7 days.
- In the last 4 Saturdays.
- In the 1st day of each month in the last 3 months.
- In the 1st day of each quarter in the last 12 months.
- In the 1st day of each year in the last 7 years.

To achieve the above example policy, configured the advanced retention policy as follows:

- Type: **Daily**
  Number of snapshots to keep: **7**

- Type: **Weekly**
  Keep retention files for the following days: **Saturday**
  Number of snapshots to keep: **4**

- Type: **Monthly**
  Keep retention files for the following days: **Day 1**
  Number of snapshots to keep: **3**

- Type: **Quarterly**

Keep retention files for the following days:
Month – January, April, July, October
Day 1
Number of snapshots to keep: **4**

- Type: **Yearly**
  Keep retention files for the following days: **01-01**
  Number of snapshots to keep: **7**

Assuming that a file is updated and being backed up everyday for the past 7 hears, and today is January 11, 2011.

If the option [Remove retention files for overlap policy] is not enabled, a total of 22 snapshots (previous version) of the file would be available for restore:

Daily	Weekly	Monthly	Quarterly	Yearly
16-Jan-2011	**14-Jan-2011**	**01-Jan-2011**	**01-Jan-2011**	**01-Jan-2011**
15-Jan-2011	**07-Jan-2011**	**01-Dec-2010**	**01-Oct-2010**	**01-Jan-2010**
14-Jan-2011	**31-Dec-2010**	**01-Nov-2010**	**01-Jul-2010**	**01-Jan-2009**
13-Jan-2011	**24-Dec-2010**		**01-Apr-2010**	**01-Jan-2008**
12-Jan-2011				**01-Jan-2007**
11-Jan-2011				**01-Jan-2006**
10-Jan-2011				**01-Jan-2005**

If the option [Remove retention files for overlap policy] is enabled, the overlapping snapshots would be removed, with the following snapshots available:

Daily	Weekly	Monthly	Quarterly	Yearly
16-Jan-2011	**14-Jan-2011**	~~**01-Jan-2011**~~	~~**01-Jan-2011**~~	**01-Jan-2011**
15-Jan-2011	**07-Jan-2011**	~~**01-Dec-2010**~~	~~**01-Oct-2010**~~	**01-Jan-2010**
~~**14-Jan-2010**~~	~~**31-Dec-2010**~~	~~**01-Nov-2010**~~	~~**01-Jul-2010**~~	**01-Jan-2009**
~~**13-Jan-2010**~~	~~**24-Dec-2010**~~		~~**01-Apr-2010**~~	**01-Jan-2008**
~~**12-Jan-2010**~~				**01-Jan-2007**
~~**11-Jan-2010**~~				**01-Jan-2006**
~~**10-Jan-2010**~~				**01-Jan-2005**

The weekly policy overrides the daily policy so the snapshots of 10-Jan-2011, 11-Jan-2011, 12-Jan-2011, 13-Jan-2011 and 14-Jan-2011 are removed.

The monthly policy overrides the weekly policy so the snapshots of 24-Dec-2010 and 31-Dec-2010 are removed.

The same applies to the monthly, quarterly and yearly policy giving a total of 11 snapshots.

Important:
The Retention Policy and Delta Merge feature is closely related, as the criteria for file merging is governed by the retention policy setting configured for a backup set.

Please refer to the Delta Merge section in this guide for further details.

6.1.9 Backup Filter

Backup Filter is a set of user defined criteria to include or exclude directories and files as backup source of a backup set.

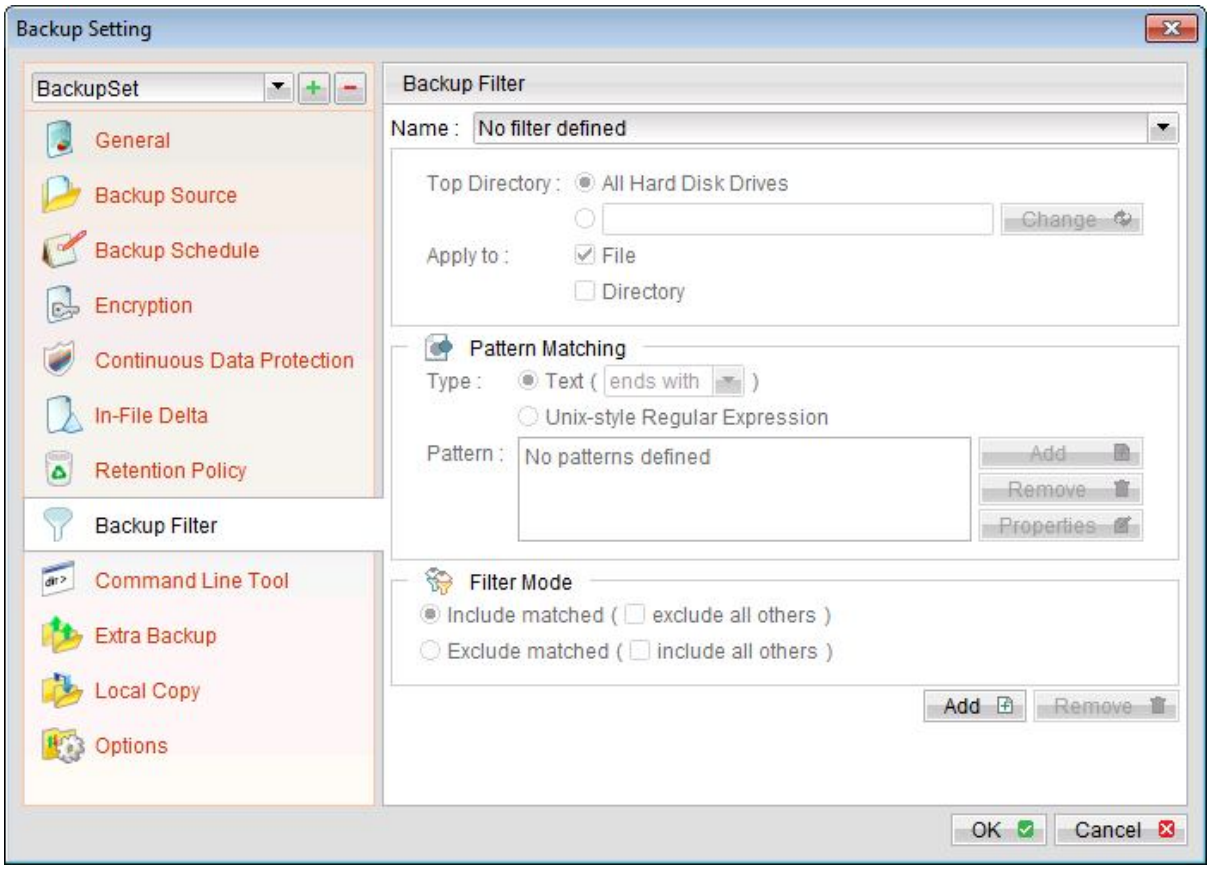
There are some basic rules regarding backup filters:

1. Filters are checked in creation order. Once inclusion / exclusion have been identified, the remaining filters will not be checked.

2. Inclusion / Exclusion made by filter always take precedence over backup source selections.

3. If all filters do not apply to a particular file, this file is then checked for inclusion / exclusion backup source selections.

To add a new filter, press the [Add] button at the bottom of the right panel.



Menu Item	Description
Name	**The name of a filter.**
Top Directory	**The top directory to which this filter is applied. Filtering rules will be applied to all files and/or directories under this directory.** **All Hard Disk Drives – select all local hard drives as the top directory automatically.**

Apply To	**Define whether to apply the filtering rule to files and/or directories.**
Pattern Matching	**It defines the filtering rules of a filter. A filtering rule can be one of the following types;** **[Starts With]** **Include/Exclude all files/directories with name starting with a certain pattern.** **Example:** **You can use B* to match all file with name starting with a B character.** **[Contains]** **Include/Exclude all files/directories with name containing a certain pattern.** **Example:** **You can use *B* to match all files with name containing with a B character.** **[Ends With]** **Include / Exclude all files / directories with name ending with a certain pattern.** **e.g. You can use *.doc to match all files with name ending with .doc (all Word Documents)** **[Regular Expression]** **Include/Exclude all files/directories with name matching a regular expression.** **To add a new pattern, press the [Add] button in the [Pattern Matching] area.** **Note: Backup filter is case sensitive.**
Filter Mode	**Defines whether you want to include or exclude matched files into/from the backup set. Also, for those unmatched files, you can choose to exclude (if include filter type) or include (if exclude filter type) them into/from the backup set.**

Example 1:

If you want to backup only Word, Excel and PowerPoint documents in your document directory (e.g. C:\My Documents), you should setup your backup filter as follows:

Top Directory = C:\My Documents
Apply To = File (true)
Matching Type = End With
Matching Patterns = *.doc, *.xls, *.ppt
Filter Mode = Include
Exclude all others = True

Example 2:
If you want to backup all files, excluding all *.exe, *.dll and *.tmp, in C:\Application, you should setup your backup filter as follows.

Top Directory = C:\Applicaitons
Apply To = File (true)
Matching Type = End With
Matching Patterns = *.exe, *.dll, *.tmp
Filter Mode = Exclude
Include all others = True

Example 3:
If you have made your selection of files (all under C:\) from the backup source setting but you want to exclude all images (e.g. *.jpg and *.gif) from your selection ,you should setup your backup filter as follows.

Top Directory = C:\
Apply to = File (true)
Matching Type = End With
Matching Patterns = *.jpg, *.gif
Filter Mode = Exclude
Include all others = false

Please note that the [Include all others] setting is not enabled because you do not want to include all other files (NOT *.jpg, *.gif) under C:\ into the backup set.

Example 4:
If you want to include everything, except the “log" directory, under C:\Applications into a backup set, you should setup your backup filter as follows.

Top Directory = C:\Applications
Apply To = Directory (true)
Matching Type = Regular Expression
Matching Patterns = ^log$
Filter Mode = Exclude
Include all others = True

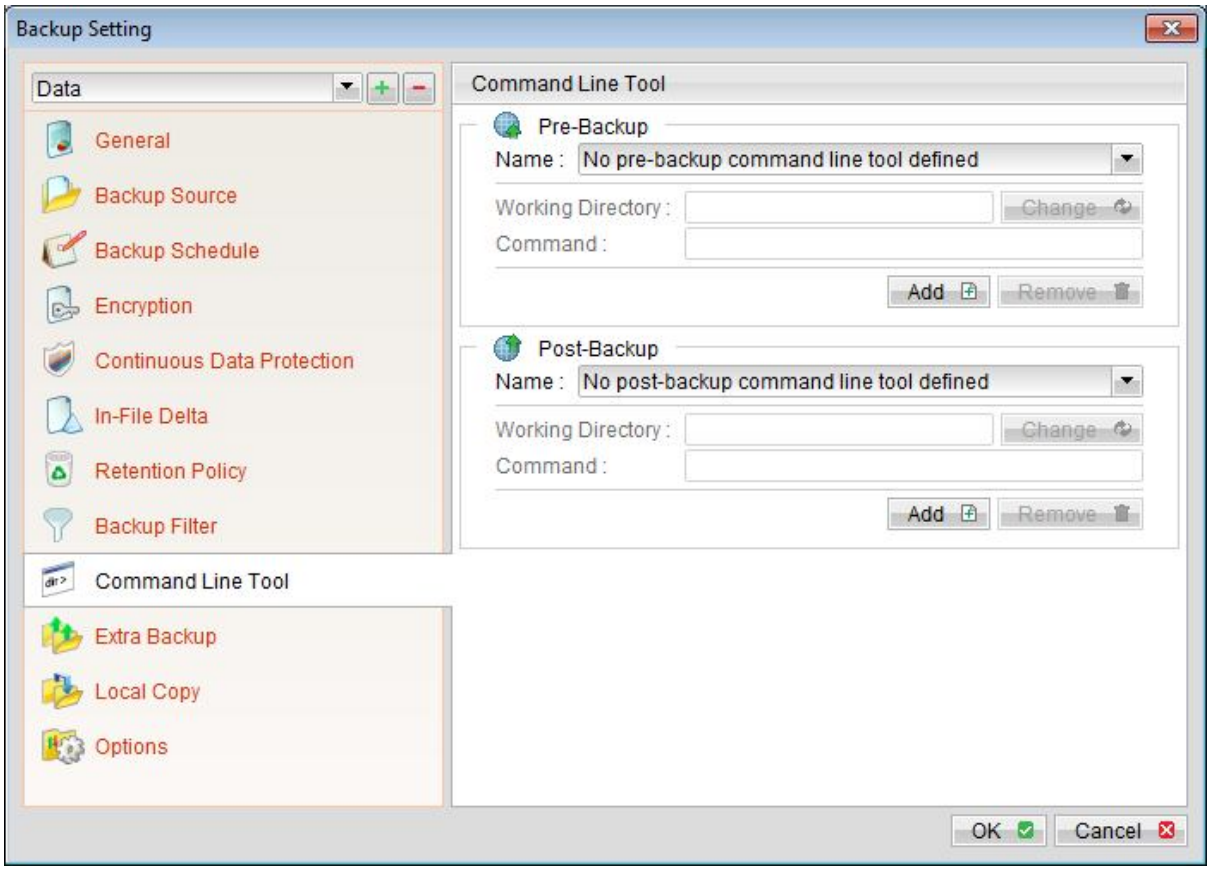
Example 5:
If you want to include all directories named “log" from the backup set files with file name starting with “B" and ending with “*.doc" under C:\My Documents into the backup set, you can use a regular expression of “^B.*\.doc$" to do your selection. The filter backup can then be setup as follows.

Top Directory = C:\My Documents
Apply To = File (true)
Matching Type = Regular Expression
Matching Patterns = ^B.*\.doc$
Filter Mode = Include
Exclude all others = True

6.1.10 Command Line Tool

Click on the [Command Line Tool] tab to configure a Pre-Backup or Post-Backup command.

Command such as batch file to stop and start an application before and after a backup job is complete, or other command such as to shutdown the computer when a backup job is complete can be configured.



Menu Item	Description
Add	**Click to add new pre or post backup command.**
Remove	**Click to remove existing pre or post backup command.**
Name	**Input box to enter name of a pre or post backup command.**
Working Directory	**Directory which the pre or post backup command will run at.**
Command	**Input box to enter pre or post backup command to be run.** **Native command or command to execute a batch file,**

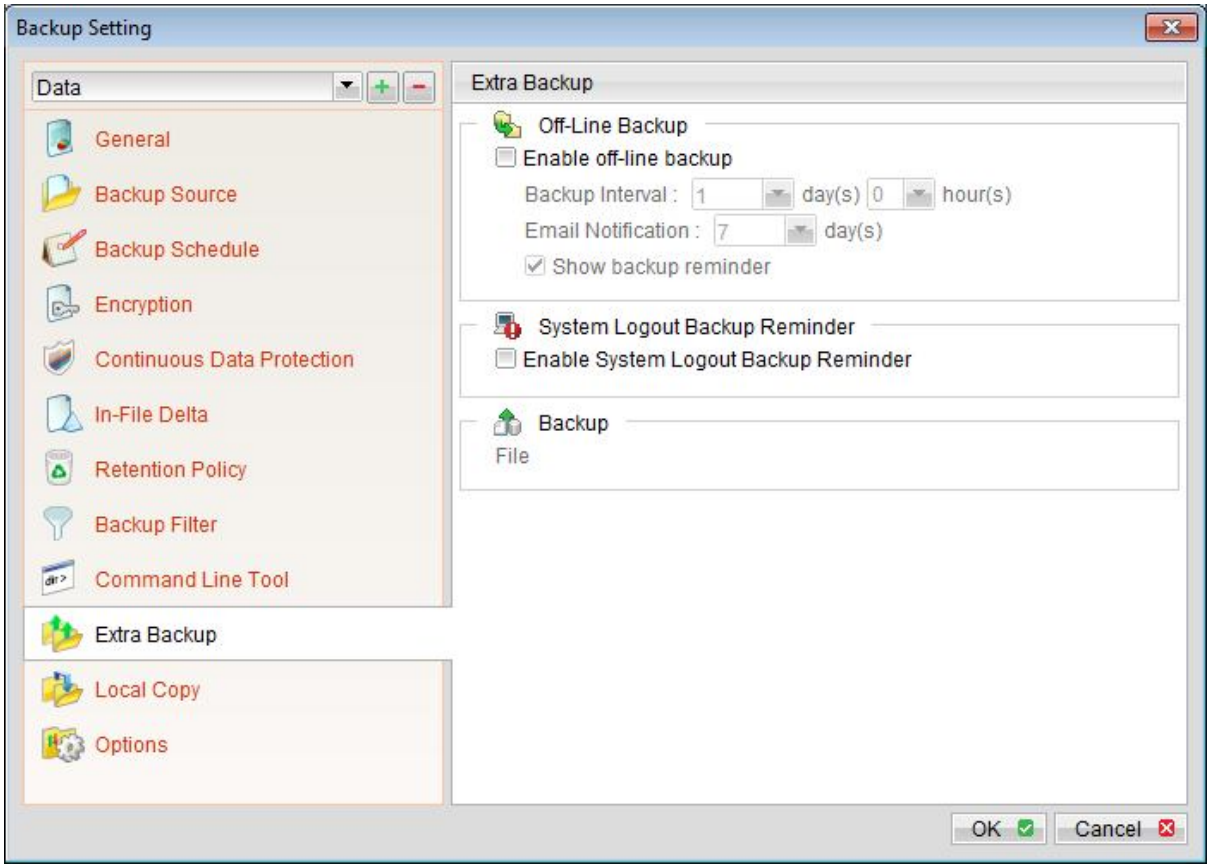
	command file, or VBScript file can be configured: **shutdown -s -t 60** **batch.bat** **command.cmd** **script.vbs** **Note: Please ensure that control is returned to the backup application once the command is executed.**

The pre and post backup command may run at different time according to the backup type. The following table outlines when they would be run:

Backup type	When does the Pre-Backup command run?	When does the Post-Backup command run?
File backup type	**Before any file is backed up (uploaded) to the backup server.**	**When the backup (upload) of all files are completed.**
Non-file backup type	**Before any database file is spooled to the designated temporary directory.**	**After spooling backup files to temporary directory (i.e. before the first backup file is uploaded).**

6.1.11 Extra Backup

Click on the [Extra Backup] tab to enable the Off-Line Backup and System Logout Backup Reminder option.



6.1.1.11 Enable off-line backup

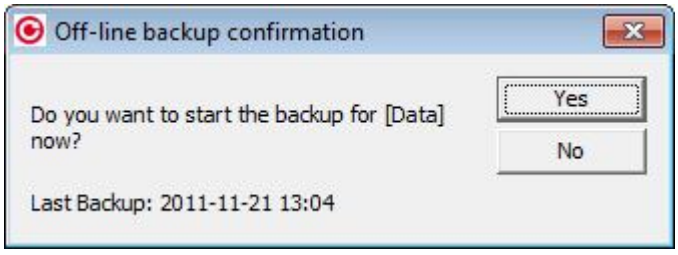
Enable off-line backup defines whether to enable the [off-line backup] feature.

The [off-line backup] feature is designed for notebook users who may be off-line most of the time, and cannot rely on backup scheduled for regular backup of their data.

Enable off-line backup	Action
Enabled	Prompt for backup if the time between the last backup to the current time exceeded the [Backup Interval].
Disabled	Do not prompt for backup.
Backup Interval	Time interval between each backup job.
Email Notification	Time interval when email would be sent for backup reminder.
Show backup reminder	To display or hide the confirmation dialog for backup. If the confirmation dialog is disabled, backup will be performed automatically when connection to the Internet is re-established.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

With the [off-line backup] setting is enabled, when the computer is connected online and the time between the last backup to the current time elapsed the [Backup Interval], a pop up off-line backup confirmation menu will be prompted, reminding the user to perform a backup.



Menu Items	Description
Yes	Perform the backup job immediately.
No	Do not perform the backup job.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

6.1.2.11 Enable System Logout Backup Reminder

Enable System Logout Backup Reminder defines whether to enable the [System Logout Backup Reminder] feature.

Enable System Logout Backup Reminder	Action
Enabled	Prompt for backup before logging out or shutting down.
Disabled	Do not prompt for backup.

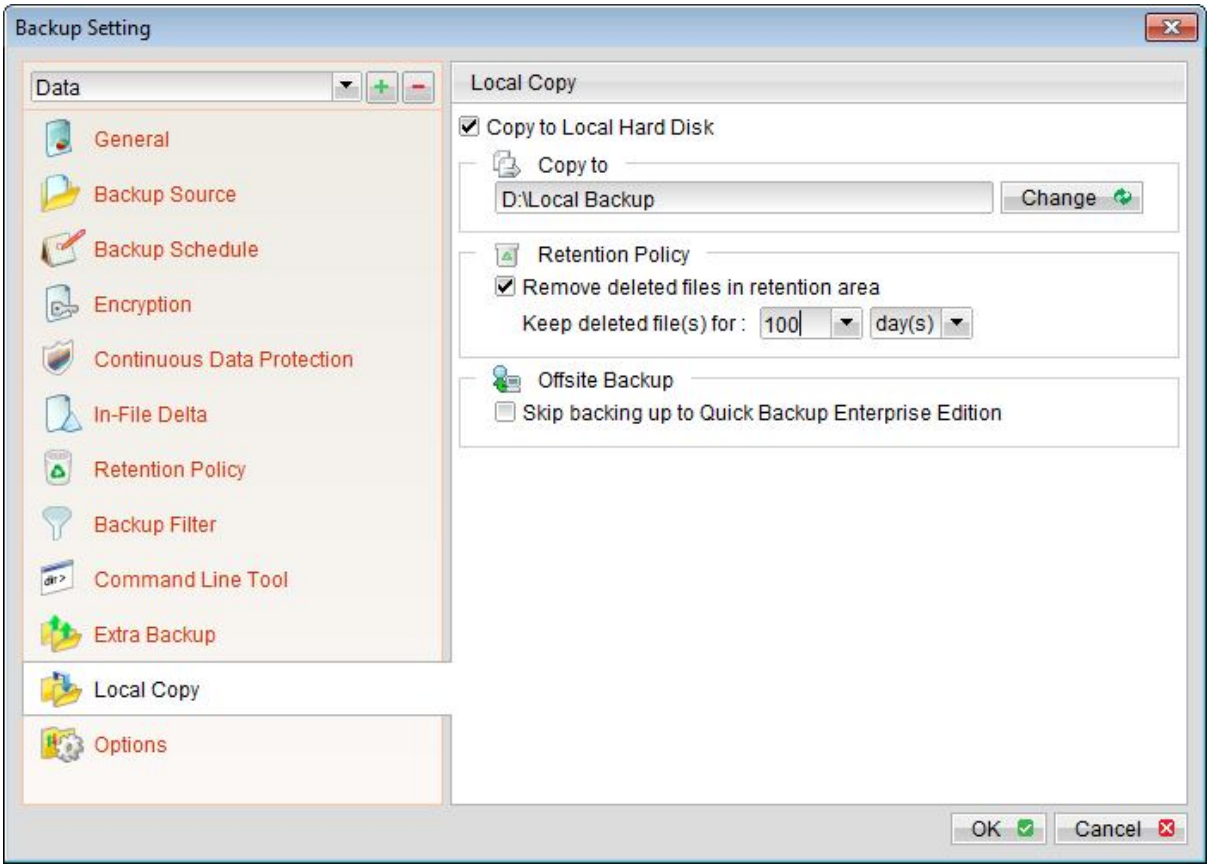
*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

When the [System Logout Backup Reminder] setting is enabled, a pop up logout reminder menu will be prompted, requesting for backup before the user logs out of the system or before shutting down Windows.

6.1.12 Local Copy

To save a copy of back up data locally on the client computer, simply enable the local copy feature of the backup client application.

Click on the [Local Copy] tab to configure a local copy backup.



Menu Items	Description
Copy to Local Hard Disk	Checkbox to enable or disable local copy backup.
Copy to	Directory which the local copy data are stored.
Remove deleted files in retention area	Checkbox to enable or disable the retention policy of the local copy backup.
Keep deleted file(s) for	Dropdown menu to select a basic retention policy. Note: For local copy backup, only basic retention policy can be applied.
Skip backing up to Quick Backup Offsite Backup Server	Checkbox to skip or to perform off-site backup for the corresponding backup set.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Select the corresponding backup set from the drop down menu, and click on the [Local Copy] tab.

Select the checkbox beside [Copy to Local Hard Disk], click the [Change] button and browse to the directory path which you would like to store the local copy backup.

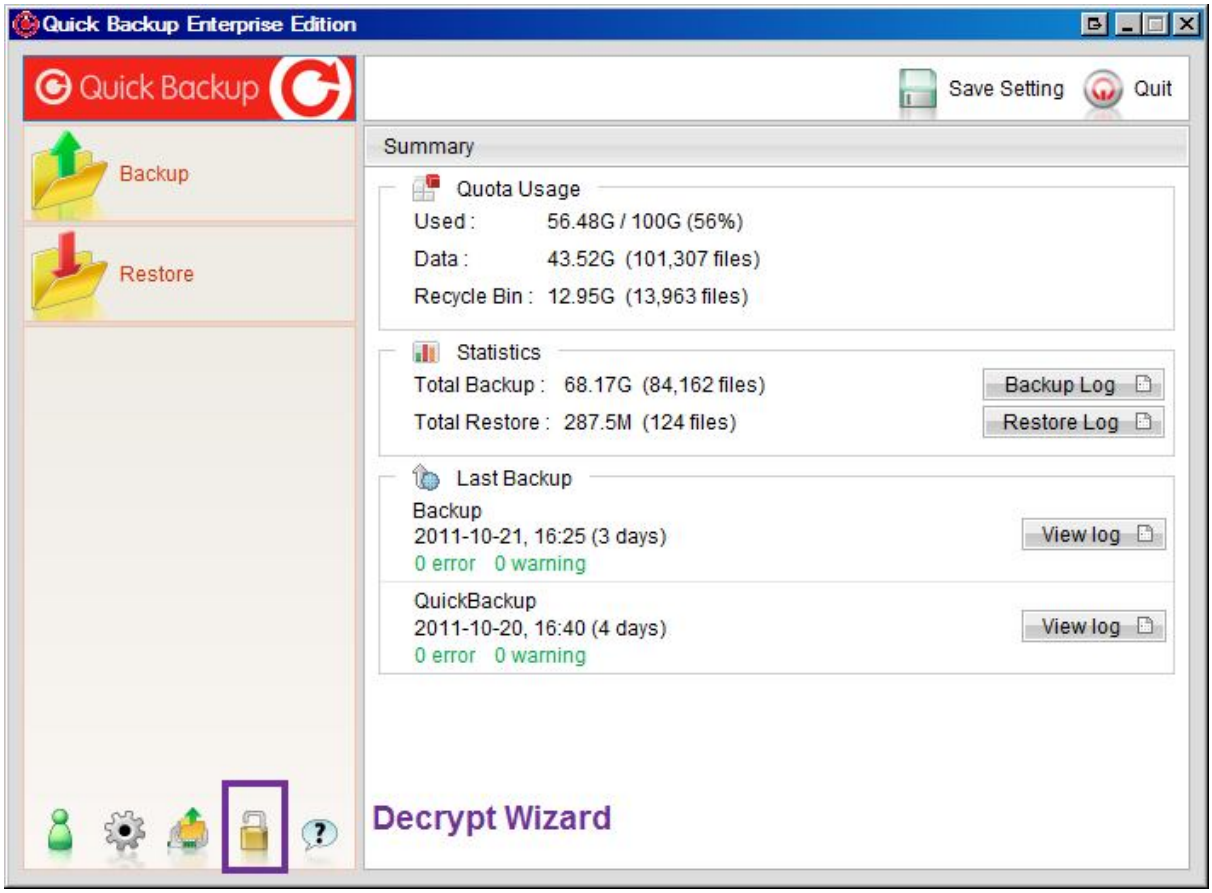
You can enable retention policy for the local copy backup (if necessary). However, note that only basic retention policy can be configured for local copy.

Retention policy of the local copy backup is separate from the retention policy configured for the off-site backup (configured in the [Retention Policy] tab).

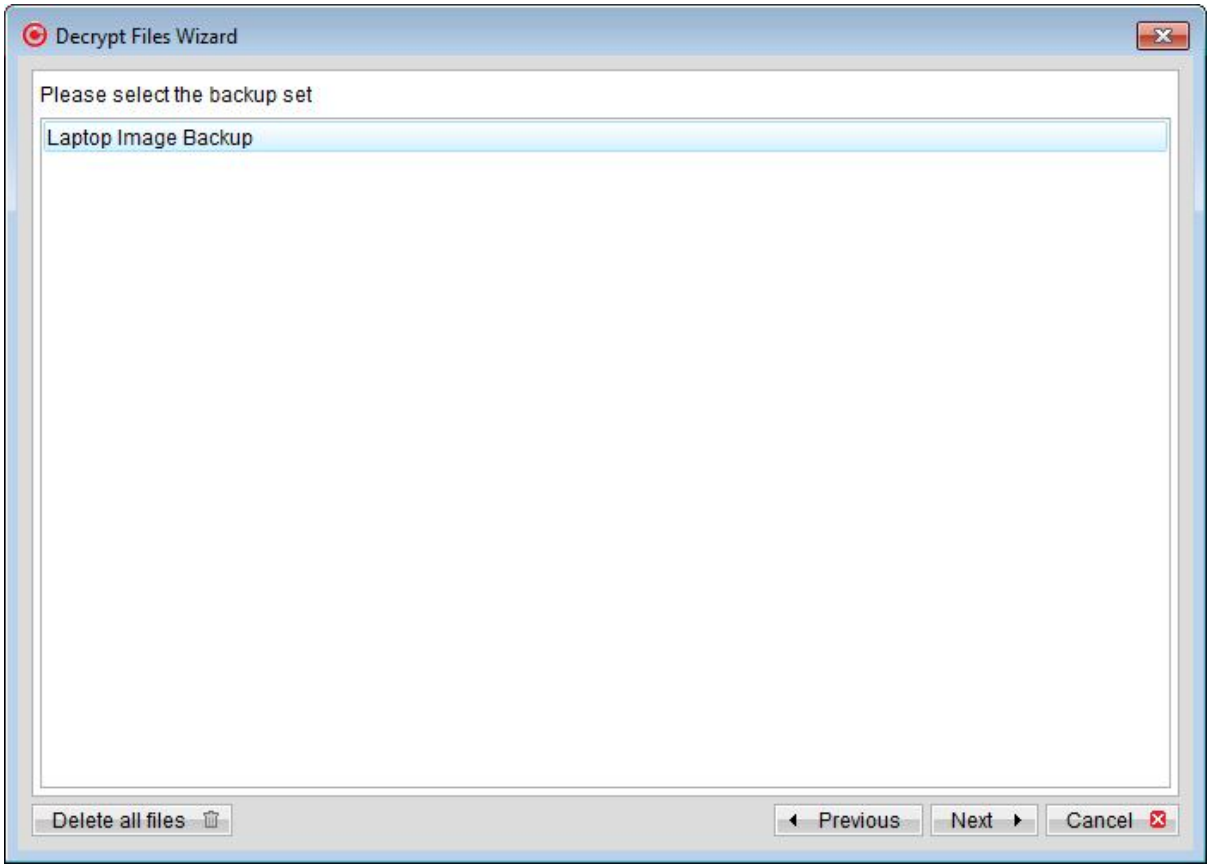
For backup set that is intended for local copy backup only, select the checkbox beside [Skip backing up to Quick Backup Offsite Backup Server].

Data that are backed up by the local copy module are compressed and encrypted. To restore local copy backed up files, please refer to the following instruction:

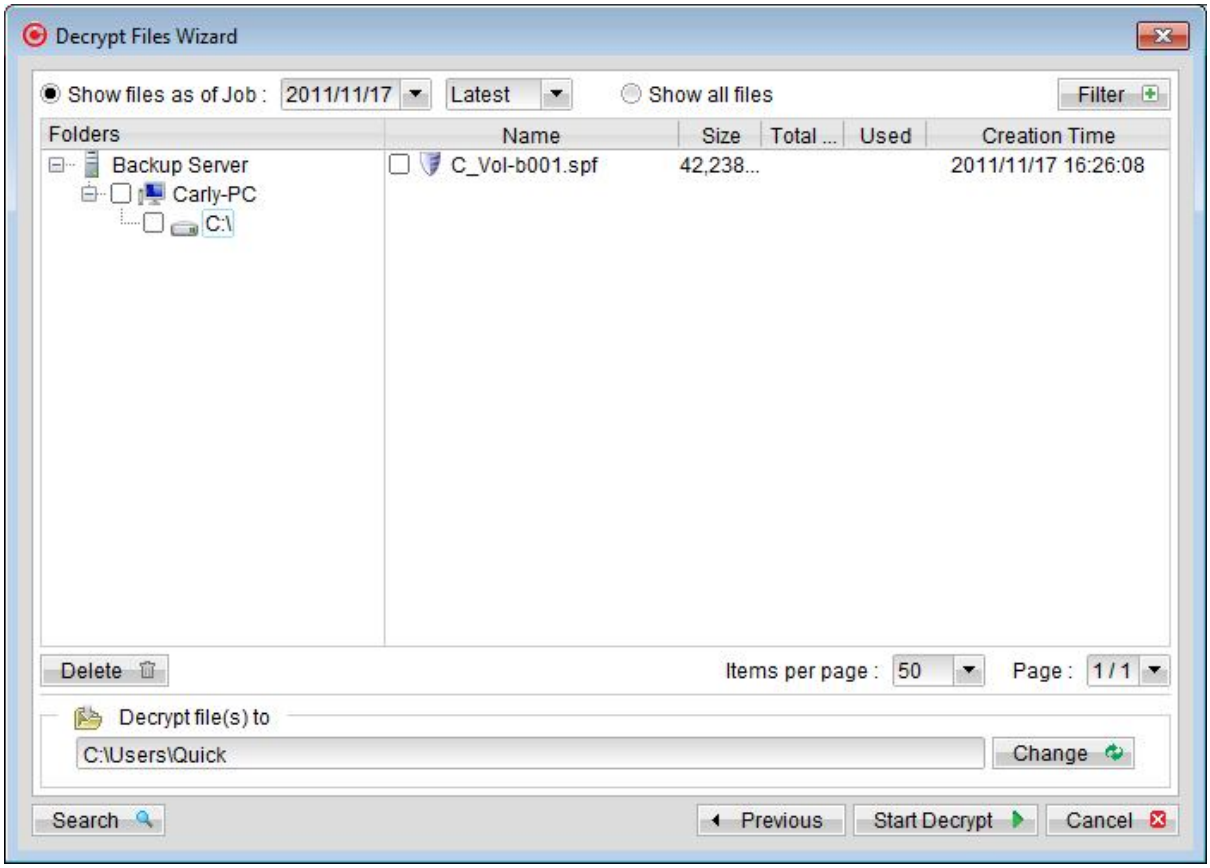
1. Press the [Decrypt Local Copy Wizard] button on the backup application's main window.



2. Select the backup set to be restored and press [Next] to proceed.



3. Follow the normal restore procedure for restoration of your local copy backed up data. For more details, please refer to Chapter 8 of this guide.



6.1.13 Temporary Directory

If you are running a file backup job with in-file delta enabled or a database type backup job, Quick Backup will generate temporary files and the directory that will be used to store all these files are defined by [Options] -> [Temporary directory for storing backup files]. Please set this to a non-system disk partition that has enough free space to avoid problems.

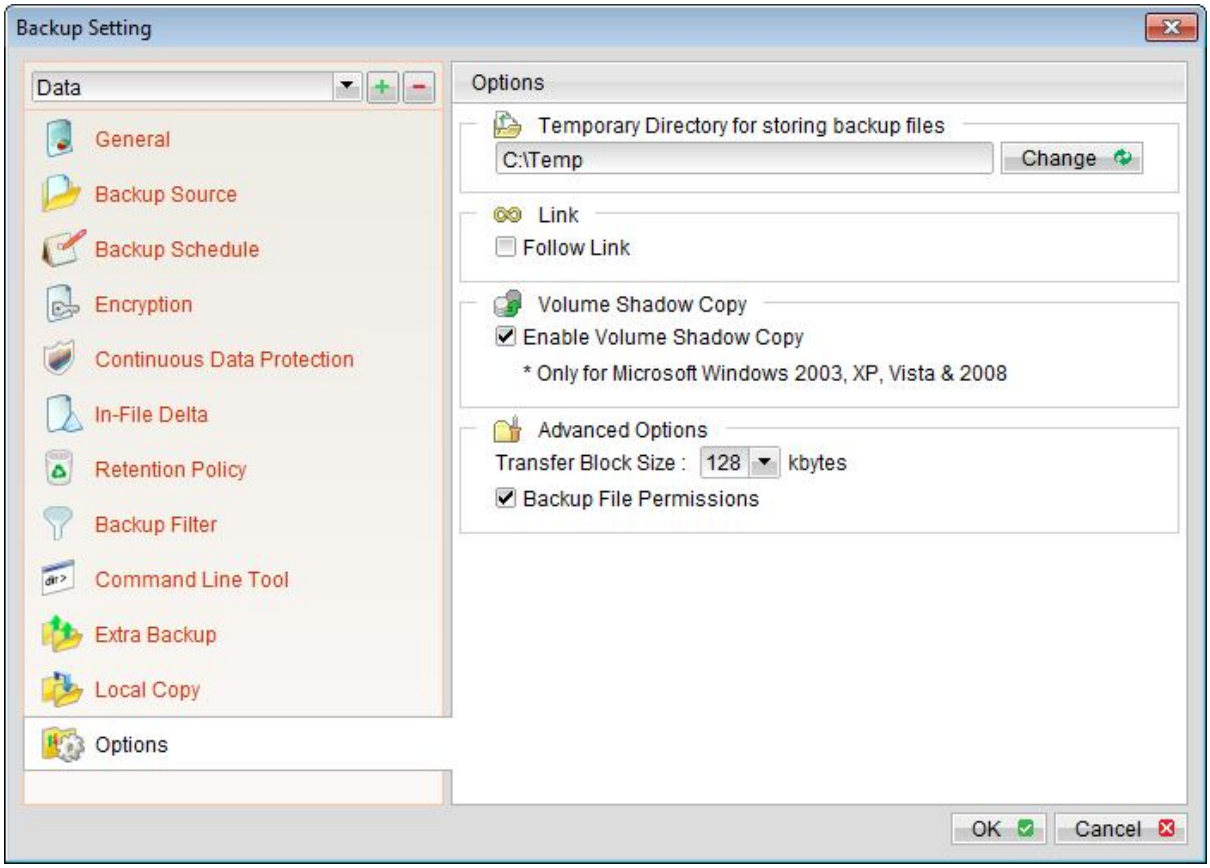
You can set the [Temporary Directory for storing backup files] to a mapped network drive. If you choose to do this, please use a UNC path (e.g. \\Server\SharePath).

6.1.14 Options

Click on the [Options] tab to configure options such as temporary directory for storing backup files, follow link, Volume Shadow Copy or advance option such as the transfer block size.

6.1.1.14 Temporary Directory for storing backup files

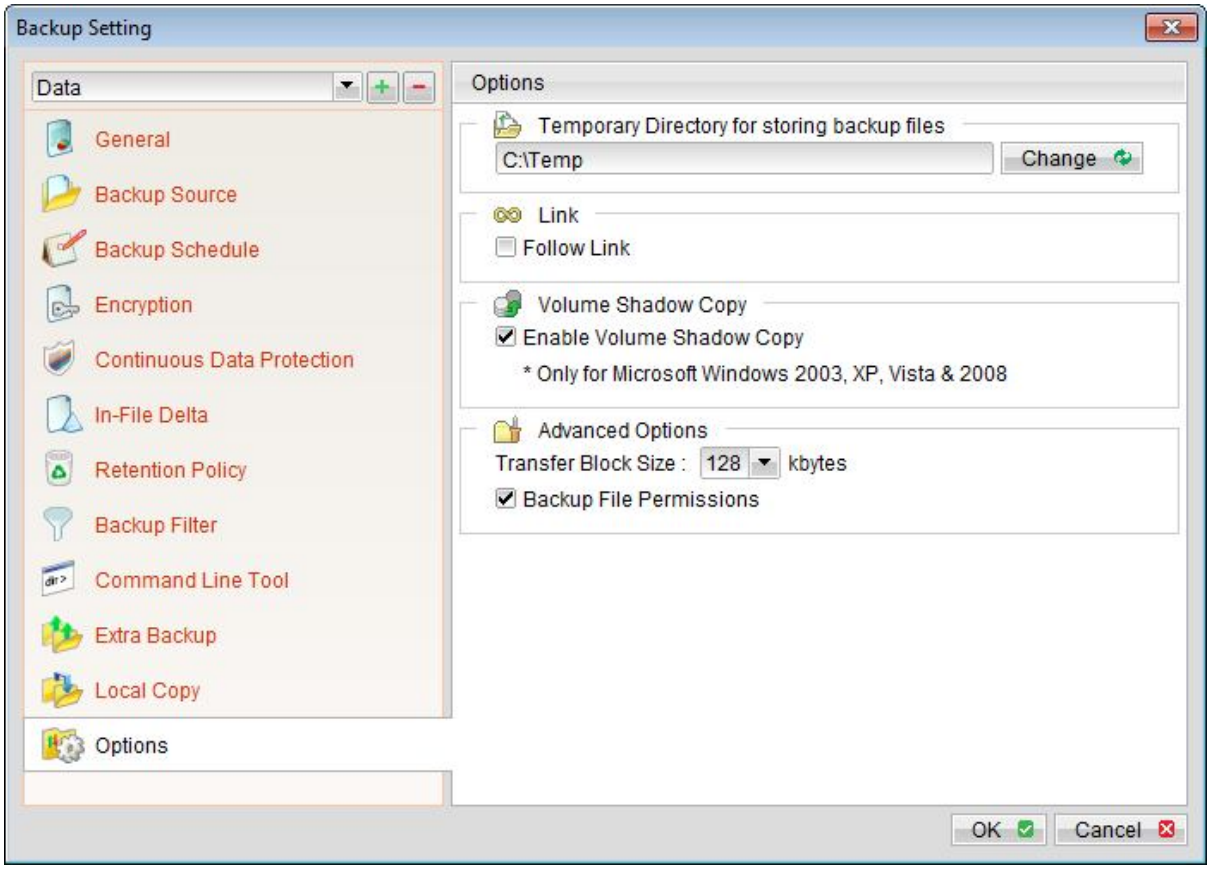
The temporary directory is used for various purposes, such as storage of temporary spooled file (for database specific backup type), remote file list, local file list, temporary delta file and other files of temporary nature.



To configure the [Temporary Directory for storing backup files], click on the [Change] button and browse to the directory path which you would like to store the temporary data.

6.1.2.14 Follow Link

Follow Link defines whether to follow an NTFS junction point or NTFS symbolic link during backup.



Follow Link	Action
Enabled	Backup junction point or symbolic link as well as the directories and files that it links to (even if the target data are not located under the backup source).
Disabled	Backup junction point or symbolic link only.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

When the follow link option is enabled, not only is the symbolic link or junction point backed up, but directories and files that the junction point links to will also be backed up.

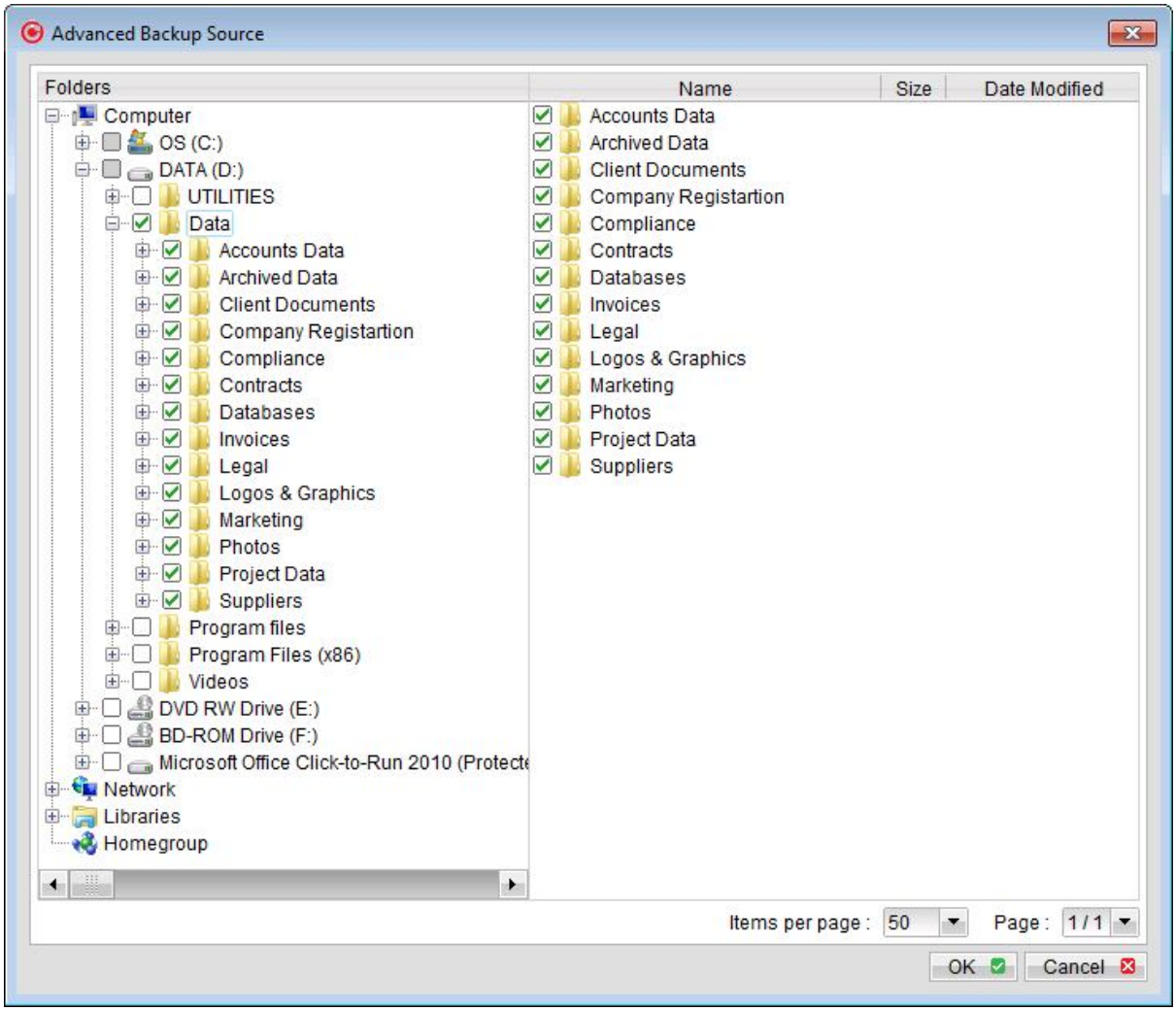
Restore outcome would be different with the different setting used during backup and during restore (e.g. there is a follow link option for backup and a follow link option in the restore menu).

The following table summarizes the outcome when a restore is performed with different options:

Follow Link	Restore to	Action
Enabled	Original Location	Junction points are restored to the original location. Restore follow link option enabled - Target directories and files are restored to the original location. Restore follow link option disabled - Target directories and files are not restored.
	Alternate Location	Junction points are restored to the location specified. Restore follow link option enabled - Target directories and files are restored to the location specified. Restore follow link option disabled - Target directories and files are not restored.
Disabled	Original Location	Junction points are restored to the original location. No data is restored to the junction point's destination.
	Alternate Location	Junction points are restored to the location specified. No data is restored to the junction point's destination.

To enable the [Follow Link] option, select the checkbox beside the follow link option

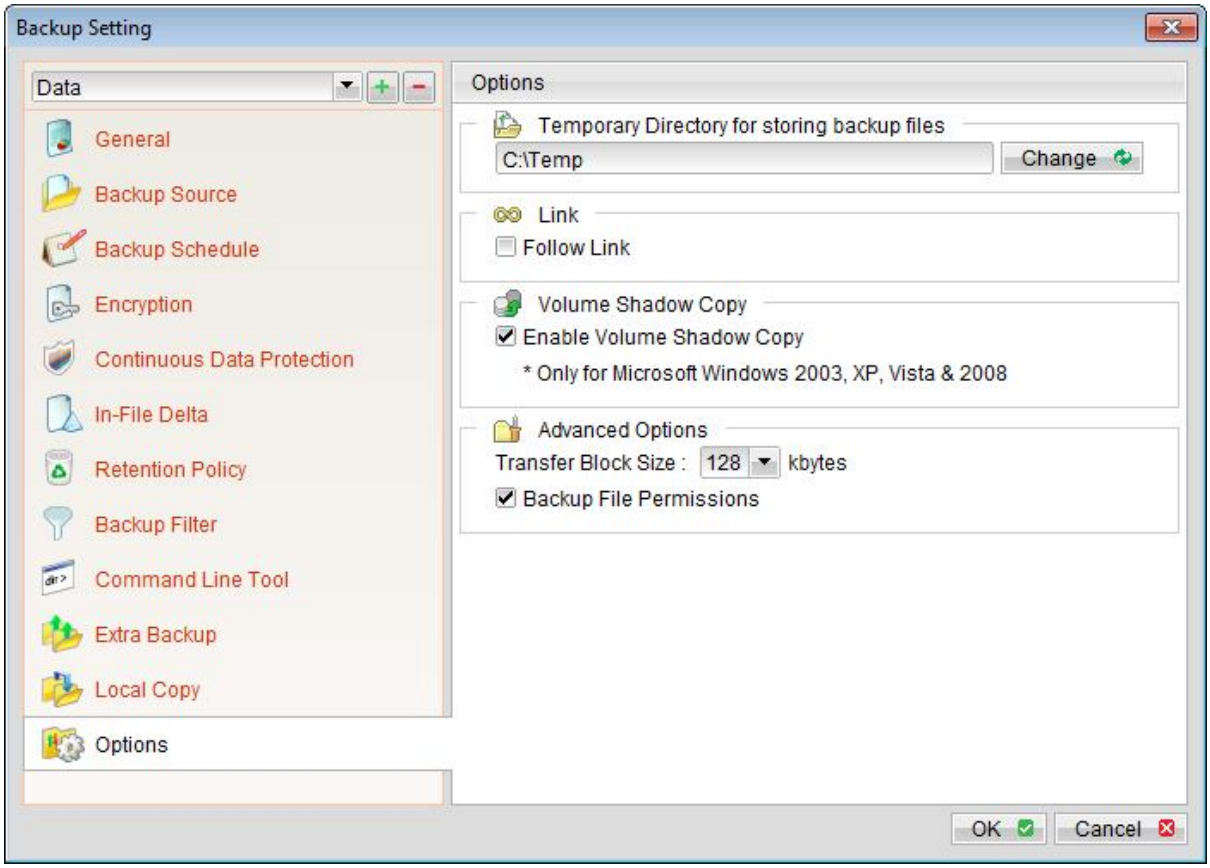
Note that system protect junction point such as the Documents and Settings junction on Windows 2008 server cannot be selected as backup source under the advanced backup source dialog (e.g. there is no select-able checkbox beside system protected junction point).



To manually select system protected junction points for backup; please select the parent directory of the junction point, or enter the corresponding junction point (e.g. C:\Documents and Settings) on the web interface.

6.1.3.14 Enable Volume Shadow Copy

Enable Volume Shadow Copy defines whether to enable Microsoft Volume Shadow Copy Service (VSS) for the backup set.



Enable Volume Shadow Copy	Action
Enabled	Create a snapshot of the data to be backed up for exclusively opened file.
Disabled	Do not create a snapshot of the data to be backed up for exclusively opened file. Error message will be shown for files that are opened during the backup process.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Enabling the Volume Shadow Copy option will allow backup of local files that are exclusively opened during the backup process (e.g. Outlook PST file).

Some requirements of the Volume Shadow Copy option include:

- Volume Shadow Copy can only be applied for local drive; exclusively opened file on network shared drive cannot be backed up even with the Volume Shadow Copy option enabled.
- Volume Shadow Copy is only available on Windows platforms released after Windows 2000 (e.g. XP / 2003 / Vista / 2008 / 7).
- The user using the backup application must have administrative privileges to access the Volume Shadow Copy service on a computer.

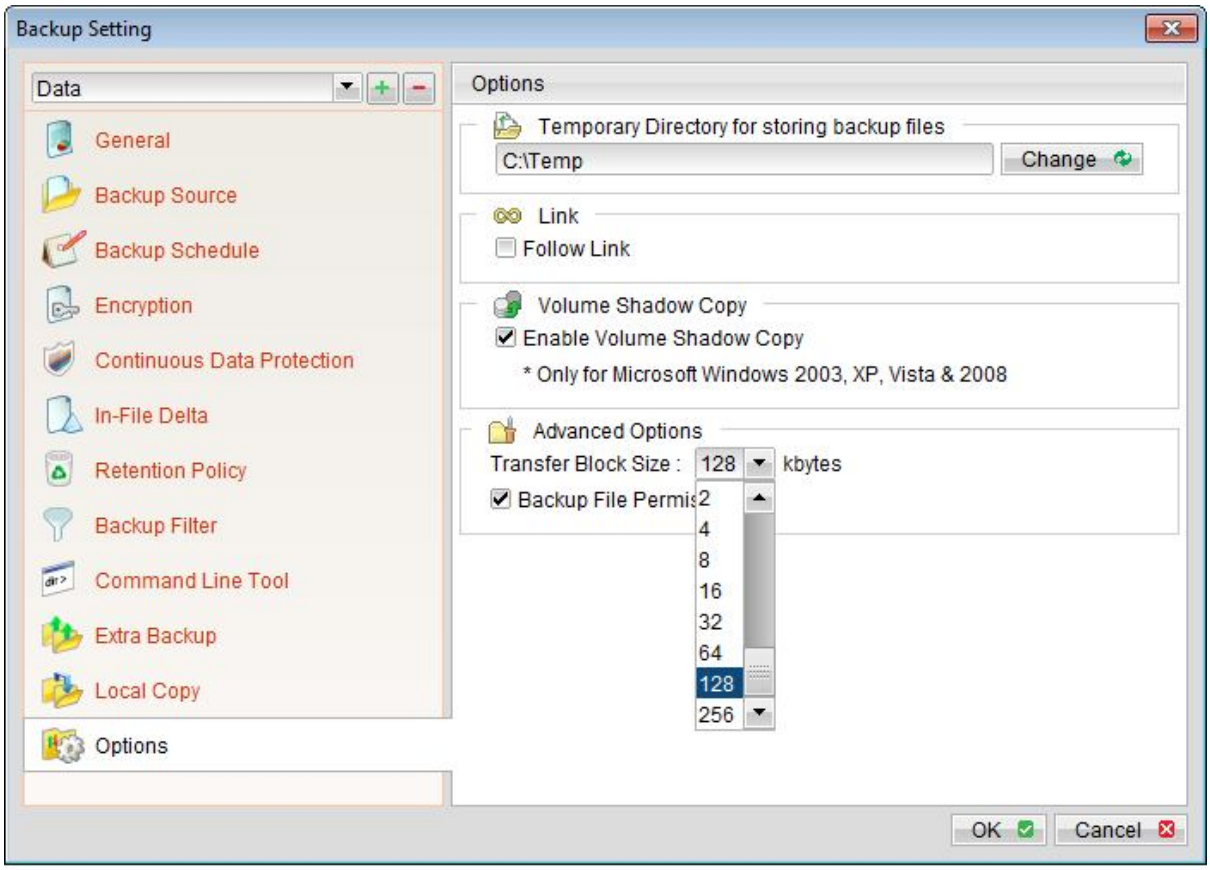
- At least one of the partitions on the machine must be in NTFS format.

For more technical information on Volume Shadow Copy, please refer to following page from Microsoft for details:

http://technet.microsoft.com/en-us/library/cc785914(WS.10).aspx

6.1.4.14 Transfer Block Size

Transfer block size defines the block size that the backup application will use to transfer your backup data to the backup server.



Note that certain firewall applications or proxy servers may block out-going network traffic with large block size for security reasons. If you are in a network with this type of restriction, please lower the transfer block size value.

To change the transfer block size of any backup set, select the [Options] tab on the left panel and then select the corresponding block size from the [Transfer Block Size] dropdown menu.

Press the [OK] button, and save before exiting out of the backup application.

6.1.5.14 Backup File Permission

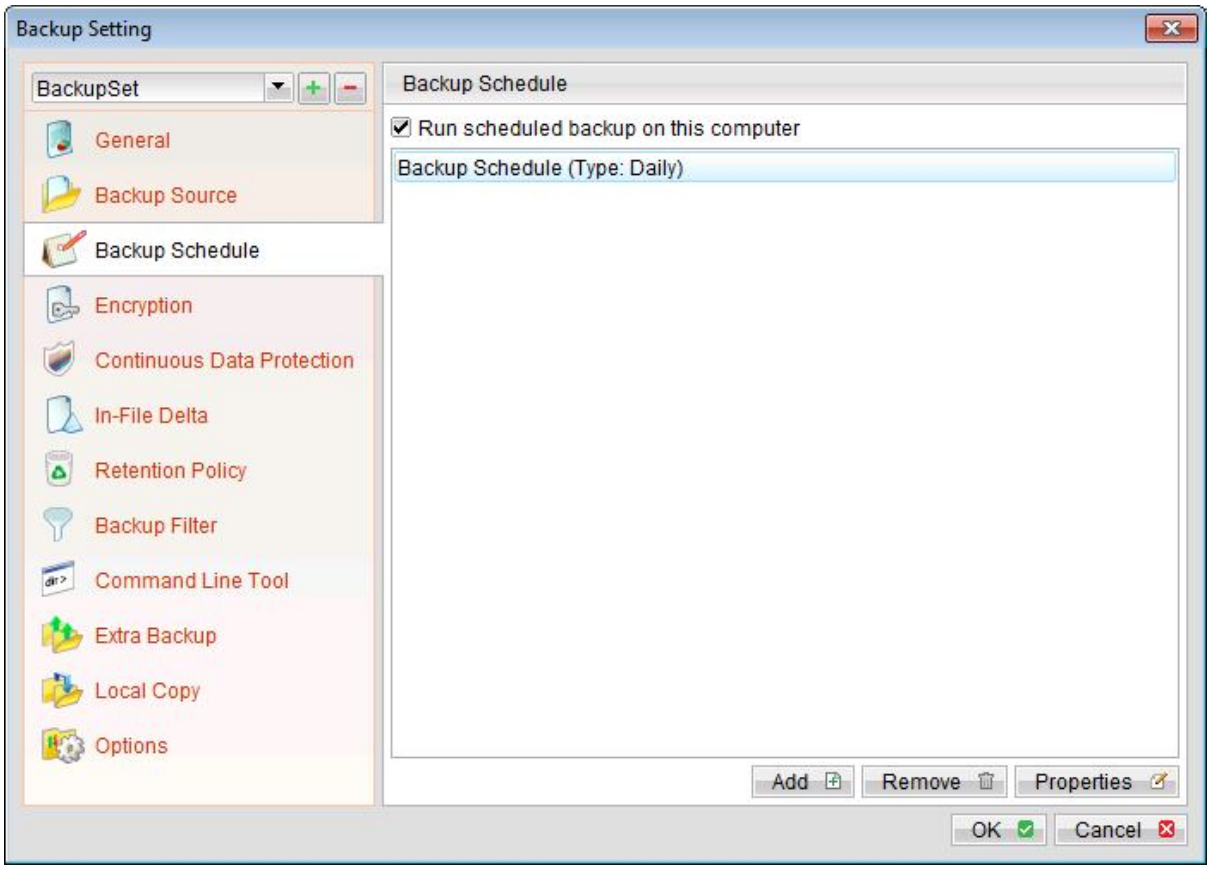
Backup file permission defines whether to backup operating system file permission of the data selected as backup source.

6.2 Single backup account for multiple computers

Multiple client computers can be backed up with a single backup user account. However, **separate backup set** must be created for **each computer**, because backup set cannot be shared.

In cases where you would like to setup a single backup account for 10 client computers. 10 backup sets must be created, with each computer having its own specific backup set for backup.

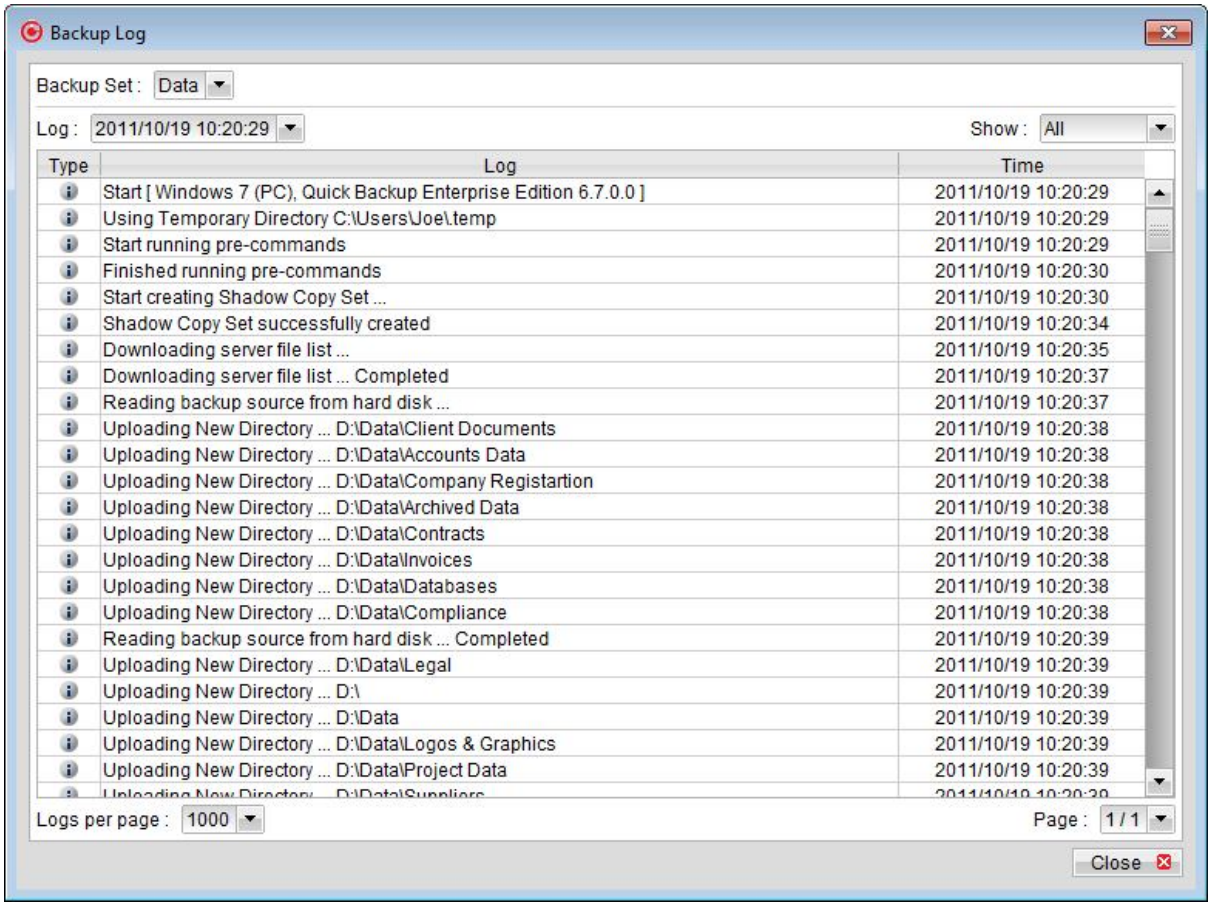
When creating backup sets in this situation, please ensure that the [Run scheduled backup on this computer] setting is properly configured for each computer. Failure to do so will result in data lost.



7 Backing Up Files

This chapter describes how to perform a backup job using the backup client application.

7.1 How data are backed up


Backup Log
Backup Set : Data
Log : 2011/10/19 10:20:29
Show : All
Type
Log
Time
Start [Windows 7 (PC), Quick Backup Enterprise Edition 6.7.0.0] 2011/10/19 10:20:29
Using Temporary Directory C:\Users\Joe\.temp 2011/10/19 10:20:29
Start running pre-commands 2011/10/19 10:20:29
Finished running pre-commands 2011/10/19 10:20:30
Start creating Shadow Copy Set ... 2011/10/19 10:20:30
Shadow Copy Set successfully created 2011/10/19 10:20:34
Downloading server file list ... 2011/10/19 10:20:35
Downloading server file list ... Completed 2011/10/19 10:20:37
Reading backup source from hard disk ... 2011/10/19 10:20:37
Uploading New Directory ... D:\Data\Client Documents 2011/10/19 10:20:38
Uploading New Directory ... D:\Data\Accounts Data 2011/10/19 10:20:38
Uploading New Directory ... D:\Data\Company Registartion 2011/10/19 10:20:38
Uploading New Directory ... D:\Data\Archived Data 2011/10/19 10:20:38
Uploading New Directory ... D:\Data\Contracts 2011/10/19 10:20:38
Uploading New Directory ... D:\Data\Invoices 2011/10/19 10:20:38
Uploading New Directory ... D:\Data\Databases 2011/10/19 10:20:38
Uploading New Directory ... D:\Data\Compliance 2011/10/19 10:20:38
Reading backup source from hard disk ... Completed 2011/10/19 10:20:39
Uploading New Directory ... D:\Data\Legal 2011/10/19 10:20:39
Uploading New Directory ... D:\ 2011/10/19 10:20:39
Uploading New Directory ... D:\Data 2011/10/19 10:20:39
Uploading New Directory ... D:\Data\Logos & Graphics 2011/10/19 10:20:39
Uploading New Directory ... D:\Data\Project Data 2011/10/19 10:20:39
Logs per page : 1000
Page : 1 / 1
Close

Stages of a backup job are outlined below:

1. A connection from the backup client application to the backup server is established.

2. A Shadow Copy set of the backup source volume is created (if available).

3. Download the server file list from the backup server.

4. Data of the backup source is compared with the server file list to compile the following file lists:

   - New file list
   - Modified file list
   - Deleted file list

5. Delta file is generated for modified file (if necessary).

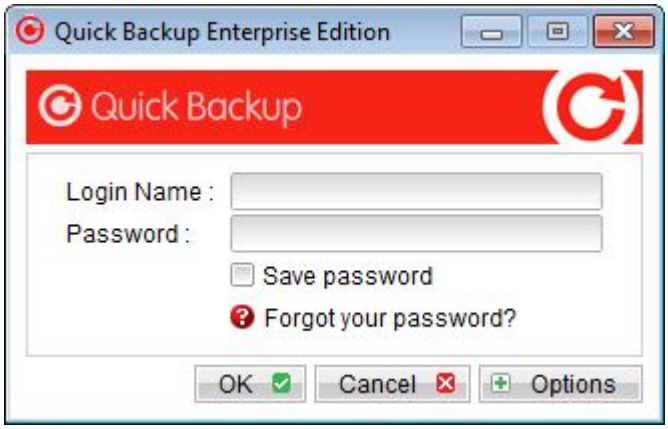
   Note: Only modified part of a file (delta file) is uploaded to the backup server, reducing the time required to complete the backup job.

6. Data are encrypted, compressed, and then uploaded onto the backup server.
7. The Shadow Copy set of the backup source is removed (if necessary).
8. Backup is completed successful.

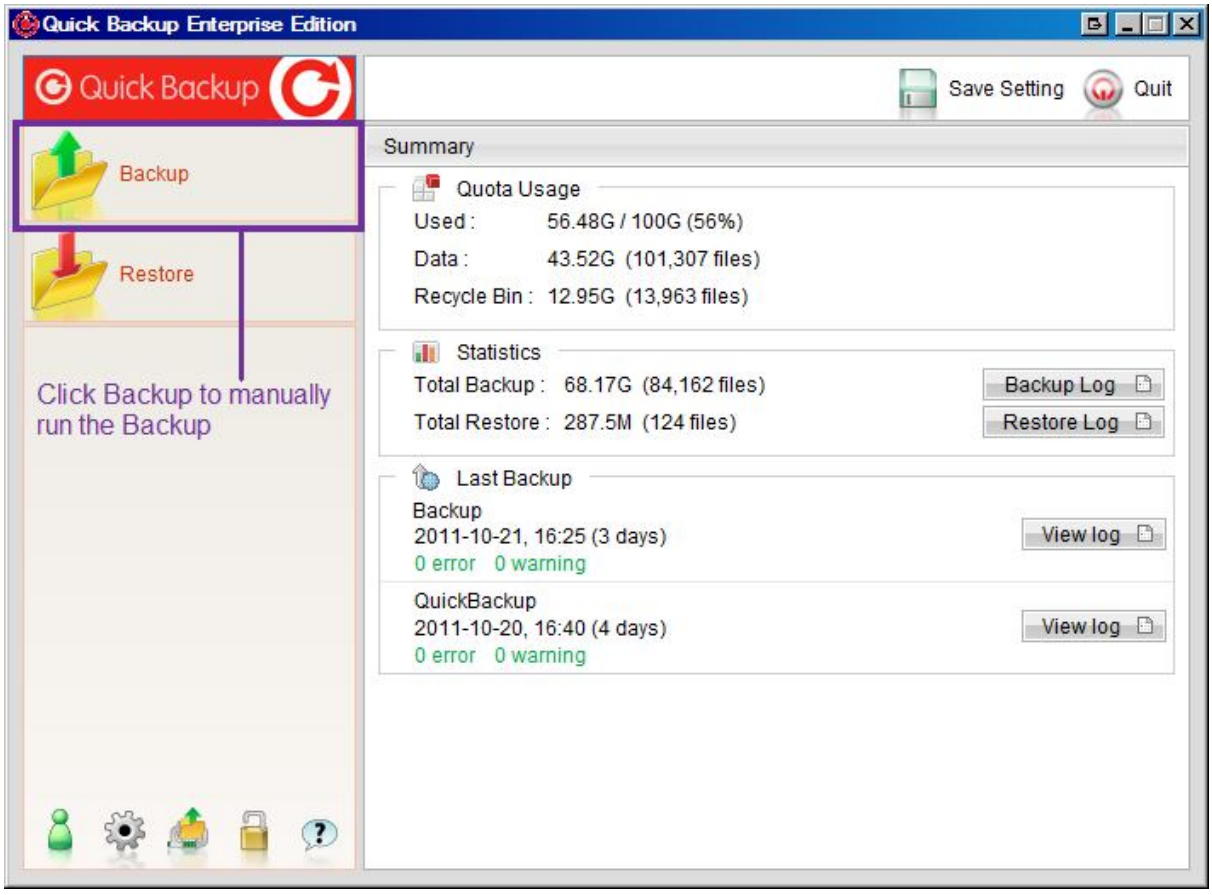
7.2 How to start an off-site backup

Please refer to the following steps for starting an off-site backup:

4. Login to the backup application's user interface.



5. Click on the [Backup] button on the backup application's main window to perform a backup manually.



6. For scheduled backup, a backup job would be automatically performed at the scheduled time specified.

Note: Scheduled backup job may be missed if the client computer is switched off, in hibernated, standby mode. Please ensure that the computer is not in the mode stated above at the scheduled backup time.

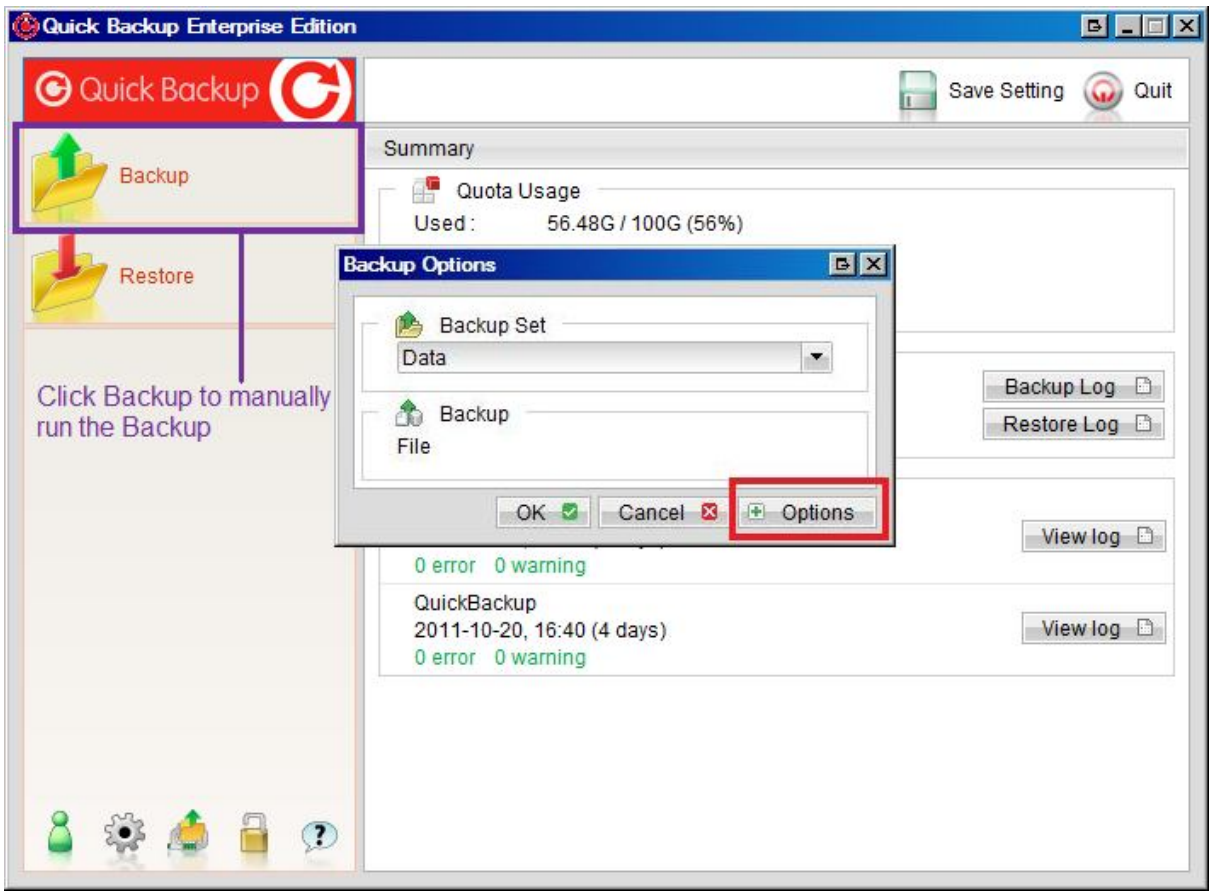
7.3 Seed Load backup

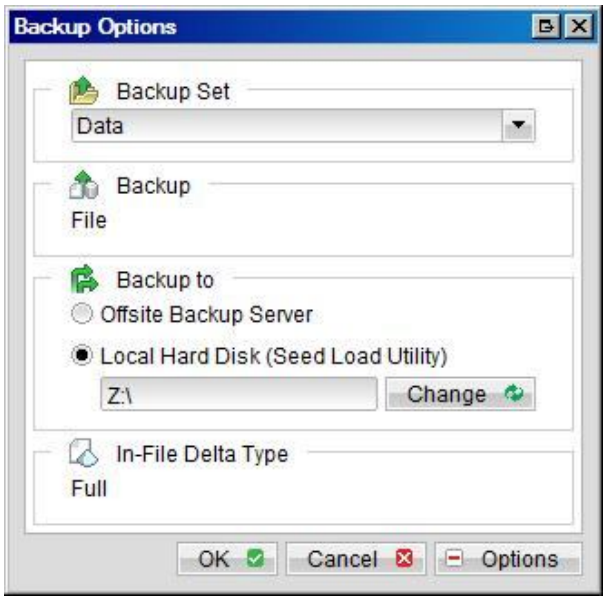
For backup of large amount of data, it would take a considerable amount of time to perform the initial full backup through the Internet.

To reduce the time and bandwidth required for initial backup, the Seed Load Utility can be utilized to perform initial backup to a local remove-able hard disk at the client site, instead of backing up through the Internet.

The backed up data can then be transported to your service provider, where they can import the data on the remove-able hard disk into your backup account on their server.

To access the Seed Load Utility, you will need to access the backup option menu:

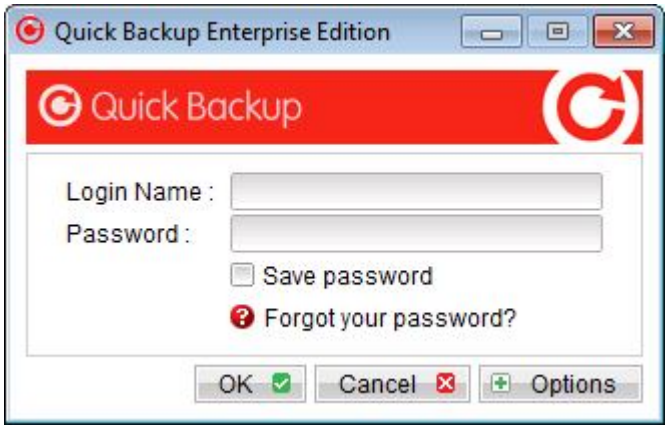




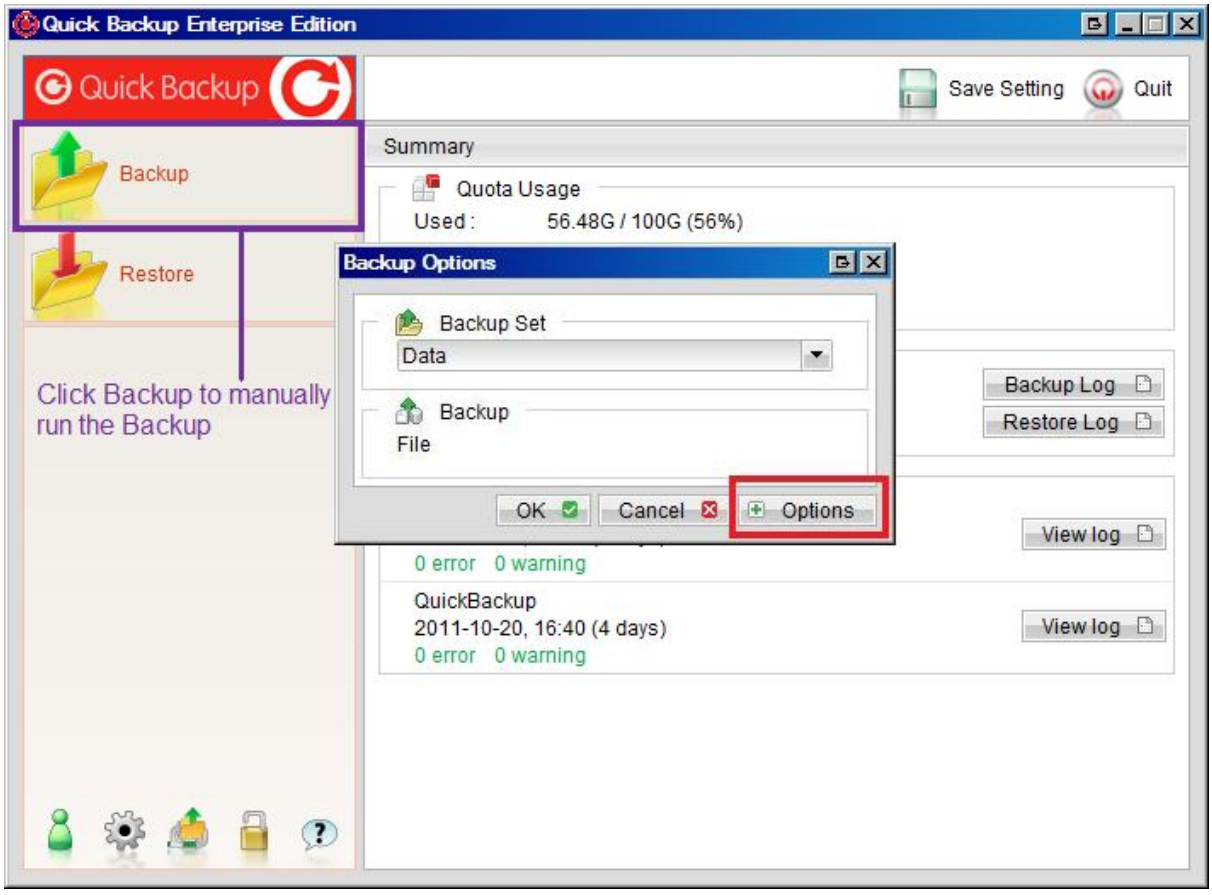
Menu Items	Description
Backup Set	Dropdown menu to select backup set.
Local Hard Disk (Local Copy)	Radio button to enable backup to local hard disk for local copy backup.
Local Hard Disk (Seed Local Utility)	Radio button to enable backup to local hard disk for seed load backup.
Change	Click to browse to the directory path which you would like to store the seed load backup.

To start a seed load backup:

1. Login to the backup application's user interface.



2. Select the [Options] button to expand the backup options menu.



Menu Items	Description
Backup Set	Dropdown menu to select backup set.
Local Hard Disk (Local Copy)	Radio button to enable backup to local hard disk for local copy backup.
Local Hard Disk (Seed Local Utility)	Radio button to enable backup to local hard disk for seed load backup.
Change	Click to browse to the directory path which you would like to store the seed load backup.

3. Select the corresponding backup set.

4. Select the radio button beside [Local Hard Disk (Seed Load Utility)].

5. Click on the [Change] button to browse to the directory path which you want the seed load data to be stored at (e.g. the remove-able hard disk).

6. Press the [OK] button to start the backup job.

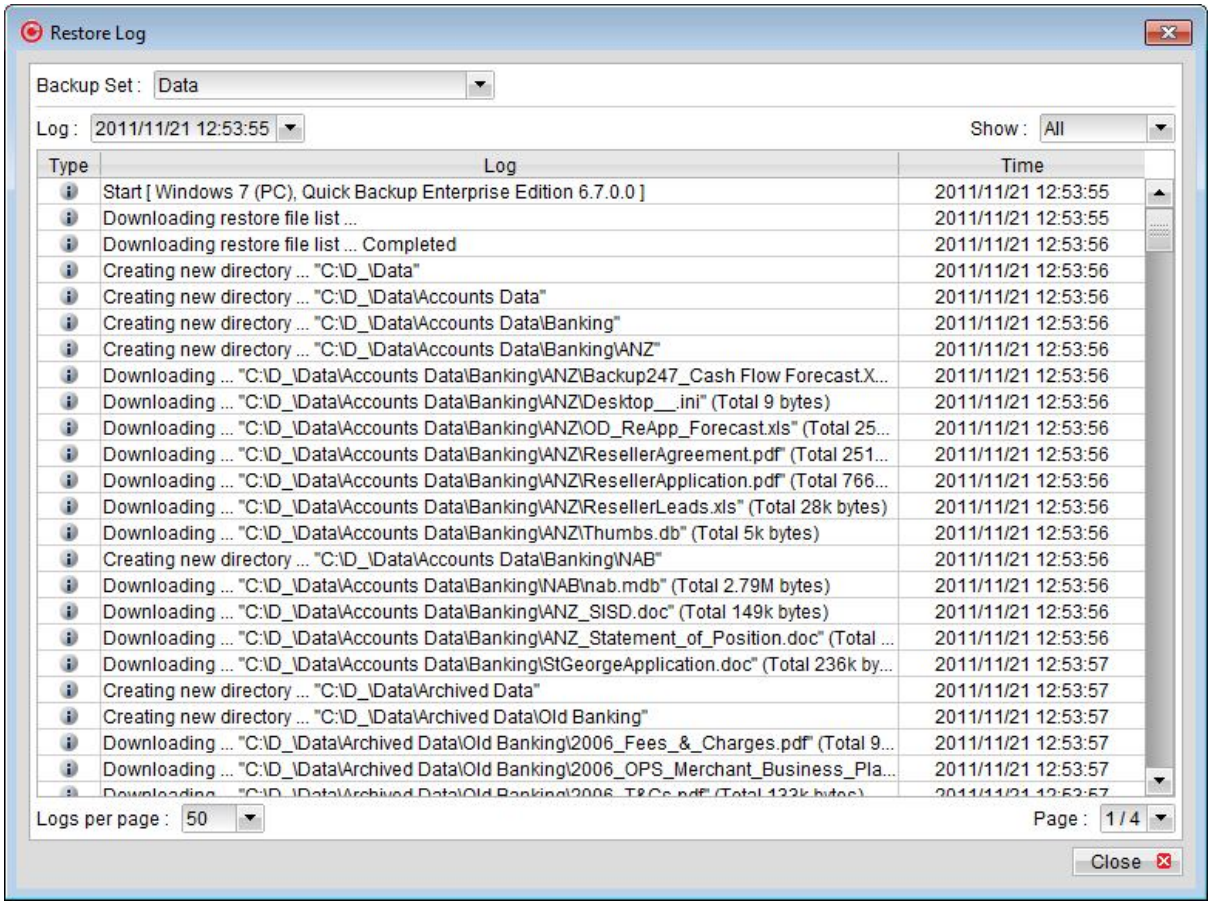
7. Send the Hard drive to Quick Backup.

Note: A seed load backup can only be performed manually.

8 Restoring Files

This chapter describes how to perform a restore using the backup client application or web console.

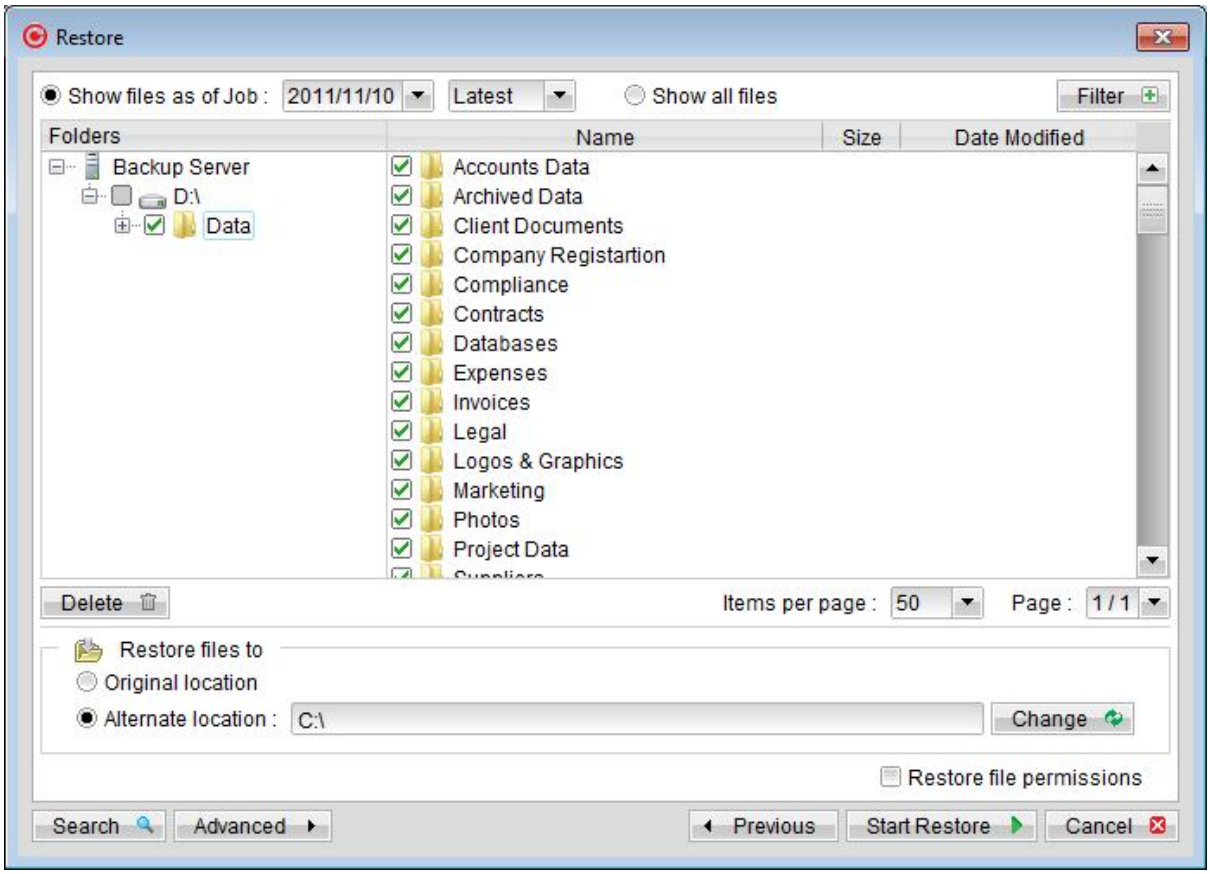
8.1 How data are restored


Restore Log
Backup Set : Data
Log : 2011/11/21 12:53:55
Show : All
Type
Log
Time
Start [Windows 7 (PC), Quick Backup Enterprise Edition 6.7.0.0] 2011/11/21 12:53:55
Downloading restore file list ... 2011/11/21 12:53:55
Downloading restore file list ... Completed 2011/11/21 12:53:56
Creating new directory ... "C:\D_\Data" 2011/11/21 12:53:56
Creating new directory ... "C:\D_\Data\Accounts Data" 2011/11/21 12:53:56
Creating new directory ... "C:\D_\Data\Accounts Data\Banking" 2011/11/21 12:53:56
Creating new directory ... "C:\D_\Data\Accounts Data\Banking\ANZ" 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ\Backup247_Cash Flow Forecast.X... 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ\Desktop__.ini" (Total 9 bytes) 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ\OD_ReApp_Forecast.xls" (Total 25... 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ\ResellerAgreement.pdf" (Total 251... 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ\ResellerApplication.pdf" (Total 766... 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ\ResellerLeads.xls" (Total 28k bytes) 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ\Thumbs.db" (Total 5k bytes) 2011/11/21 12:53:56
Creating new directory ... "C:\D_\Data\Accounts Data\Banking\NAB" 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\NAB\nab.mdb" (Total 2.79M bytes) 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ_SISD.doc" (Total 149k bytes) 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\ANZ_Statement_of_Position.doc" (Total ... 2011/11/21 12:53:56
Downloading ... "C:\D_\Data\Accounts Data\Banking\StGeorgeApplication.doc" (Total 236k by... 2011/11/21 12:53:57
Creating new directory ... "C:\D_\Data\Archived Data" 2011/11/21 12:53:57
Creating new directory ... "C:\D_\Data\Archived Data\Old Banking" 2011/11/21 12:53:57
Downloading ... "C:\D_\Data\Archived Data\Old Banking\2006_Fees_&_Charges.pdf" (Total 9... 2011/11/21 12:53:57
Downloading ... "C:\D_\Data\Archived Data\Old Banking\2006_OPS_Merchant_Business_Pla... 2011/11/21 12:53:57
Logs per page : 50
Page : 1 / 4
Close

Stages of a restore are outlined below:

1. A connection from the backup client application to the backup server is established.
2. Download the restore file list from the backup server.
3. Create the directory path for the restoration (if necessary).
4. Download the backup data from the backup server.
5. All the data will be decompressed and decrypted on the backup client computer.
6. Merging of delta files (for file with multiple delta files, if necessary).
7. Merging of combined delta file with full file.
8. Restore is completed successfully.

8.1.1 Restore Menu



Menu Items	Description
Show files as of Job	Radio button to display files available for restore as of which backup job.
[YYYY/MM/DD]	Dropdown menu to select the date of a backup job (used with the [Show files as of Job] option).
[hh/mm/ss]	Dropdown menu to select the time of a backup job (used with the [Show files as of Job] option).
Show all files	Radio button to display all files available for restore.
Filter	Click to open the filter option.
Delete	Click to delete the selected file from the backup server. **Important: Files will no longer be available for restore after they are deleted from the backup server.**
Original location	Restore directories and files to their original location.
Alternate location	Restore directories and files to an alternate location specified.

Change	Click to change the directory path of the restore destination.
Restore file permissions	Checkbox to enable or disable restore of file permission.
Search	Click to open the Search option.
Advanced	Click to open advanced option: Delete extra files - Click to synchronize the selected restore source with the restore destination during the restore process. Follow Link – Click to restore link destination's data.

*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

Select the [Show files as of Job] to display files available as of a particular backup job.

For example, to display the files available for restore since the backup job performed on 11:00am Mar 11th, 2011. Select [Show files as of Job], [2011/03/11] and [11/00/00]

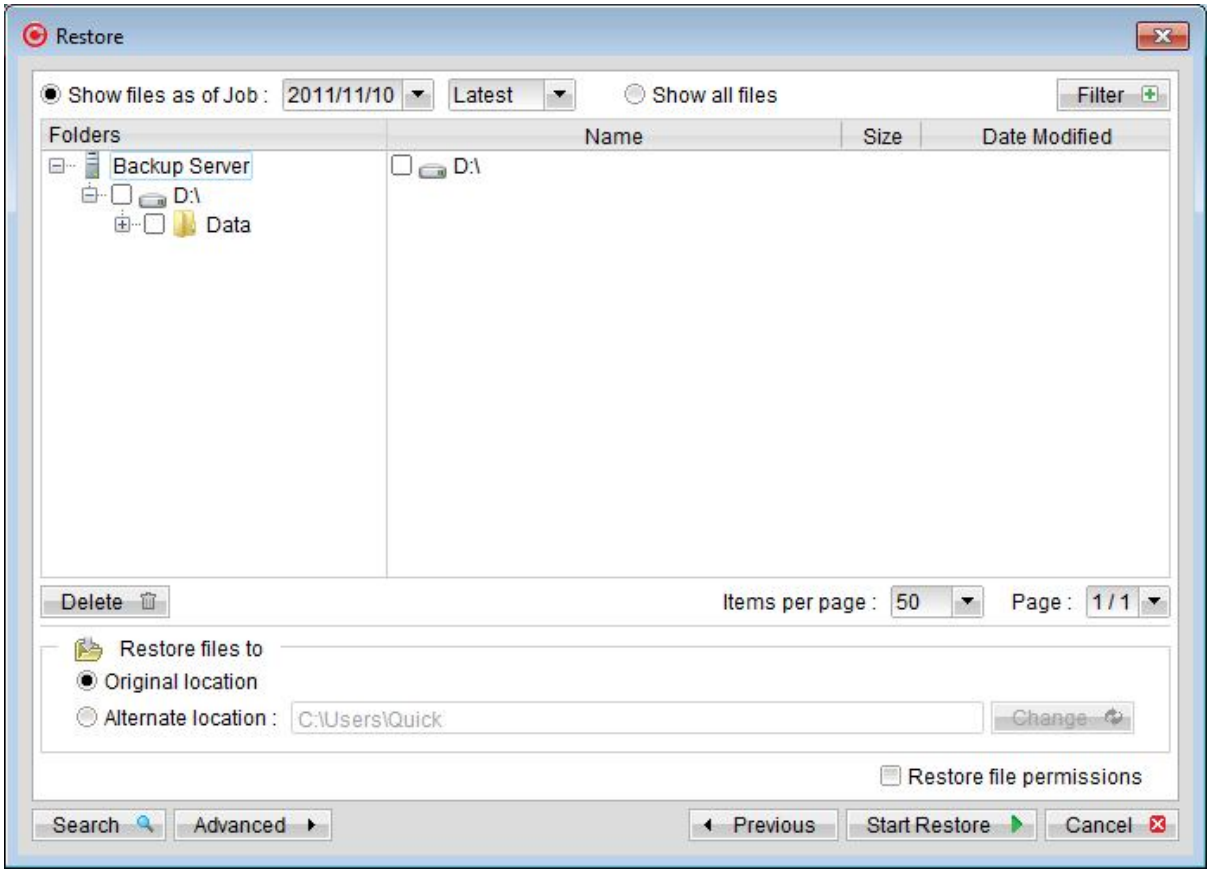
Alternatively, select the [Show all files] to display all files available for restore.

For restore to the original location on the client machine, select the [Original location] radio button.

For restore to an alternate location, select the [Alternate location] radio button, and click [Change] to change the directory path which you would like to restore to.

8.1.1.1 Filter

Click on the [Filter] button to expand the filter option.



Menu Items	Description
Pattern	Input box for entering the pattern of files that you would like to show. Note: Backup filter is case sensitive.
Type	Dropdown menu for selecting the type of pattern, they includes: [contains] [exact] [starts with] [ends with]
Match case	Checkbox to enable or disable case sensitivity.
Apply	Click to apply the filter settings.

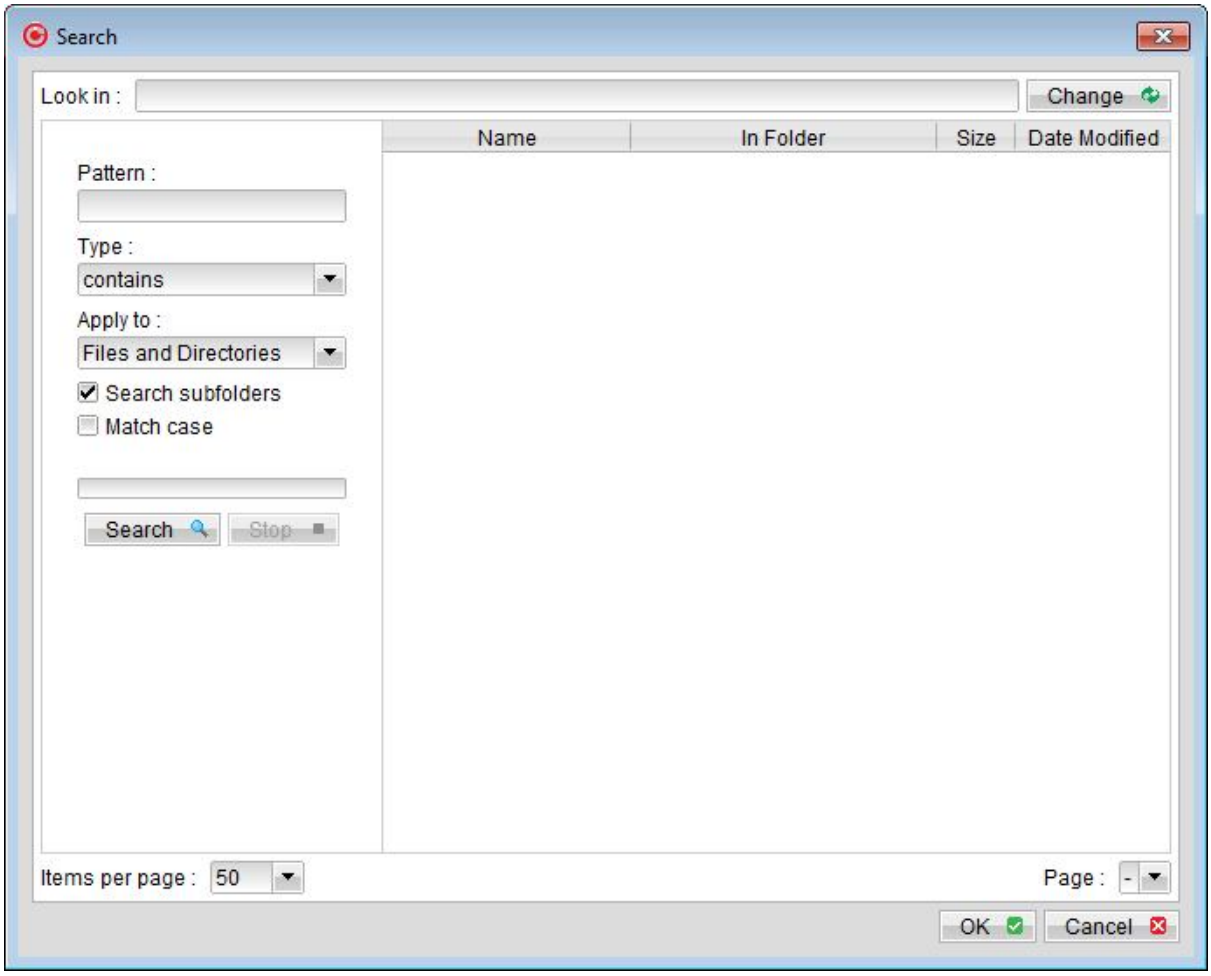
*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

The [Filter] option is useful when you want to restore only files that follow a certain pattern. For example, Microsoft Words document file that ends with .doc only.

Enter the pattern .doc into the [Pattern] textbox, select type [ends with] from the [Type] dropdown menu, and click [Apply].

8.1.2.1 Search

Click on the [Search] button to open the filter menu.



Menu Items	Description
Look in	Click on the [Change] button to browse to the search destination.
Pattern	Input box for entering the pattern of files that you would like to search for.
Type	Dropdown menu for selecting the type of pattern, they includes: [contains] [exact] [starts with] [ends with]
Apply to	Dropdown menu for selecting if the search is applied to: [Files and Directories] [Files only] [Directories]

Search subfolders	Click to enable or disable search on the subfolders of the selected [Look in] directory.
Match case	Checkbox to enable or disable case sensitivity.
Search	Click to begin the search.
Stop	Click to stop the search process.

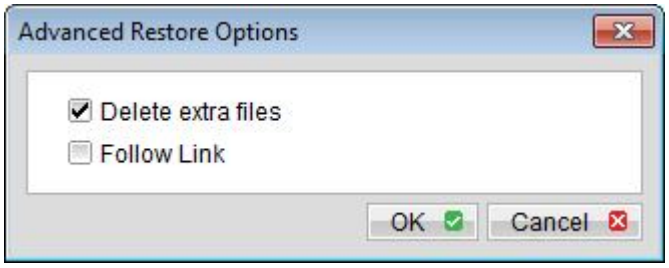
*The availability of features listed above may be service provider dependent. If a feature is not available, please check with your service provider for further details and availability.

The [Search] option can be used to locate a directory or file within a backup set with large amount of data. When the search is completed, user can select the data for restore in the search menu.

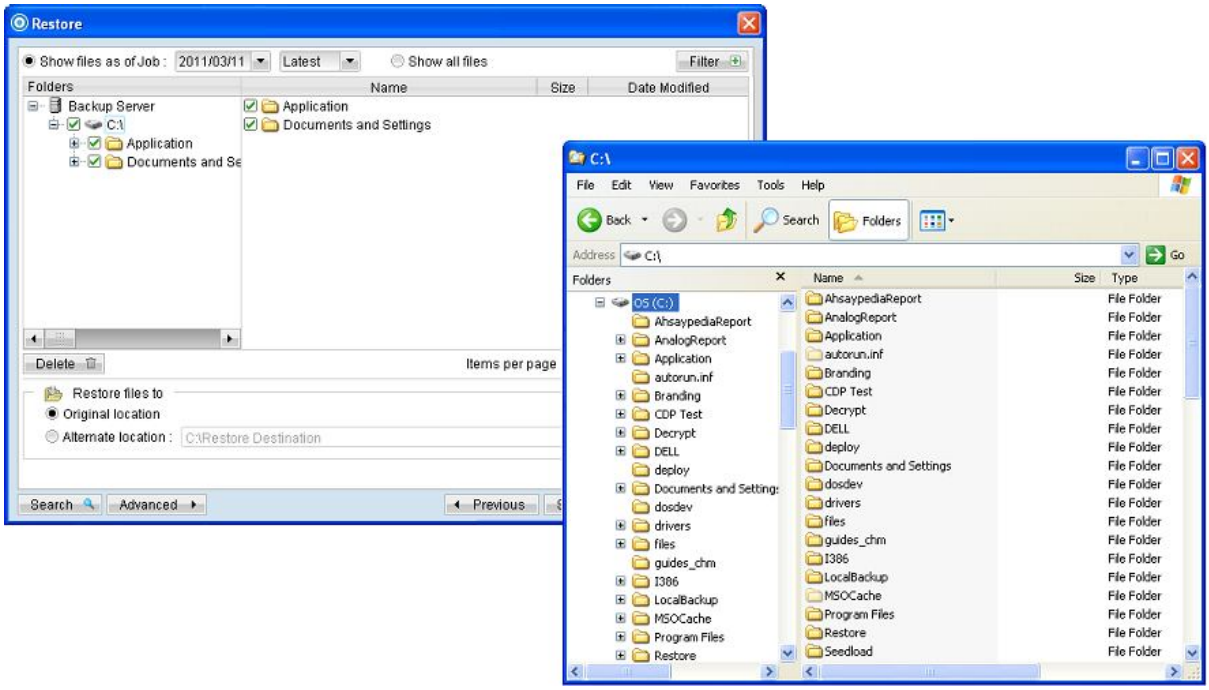
For restore that follow a certain pattern, for example, Microsoft Words document file that ends with .doc only. Enter the pattern .doc into the [Pattern] textbox, select type [ends with] from the [Type] dropdown menu, and click [Apply].

8.1.3.1 Delete extra files

Click on the [Advanced] button, select the [Delete extra files] checkbox to enable the delete extra file option.



When the [Delete extra files] option is enabled, the restore process will attempt to synchronize the selected restore source with the restore destination.

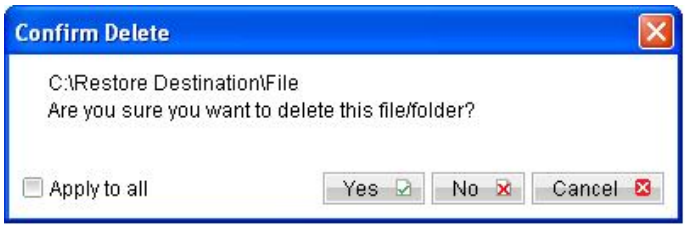


In the image above, where C:\ is selected as the restore source, and [Original location] is selected as the restore destination.

The restore process will attempt to synchronize the restore destination (current C:\ on the client machine) with the restore source (C:\ that is backed up on the backup server).

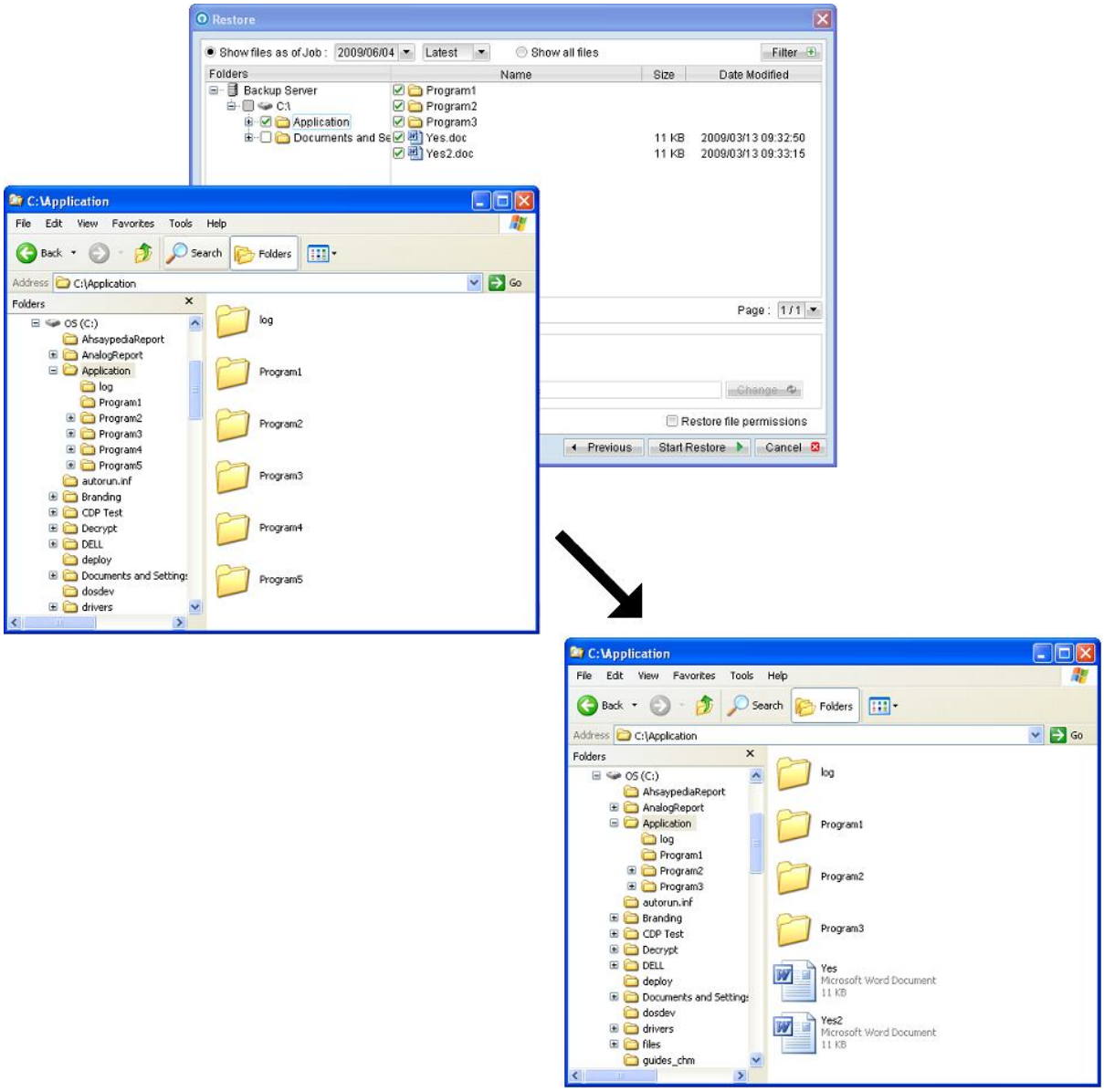
Specifically, the restore process will restore the Application, Documents and Settings folders and the data within, and then delete all other data on C:\ to mirror the restore source and destination.

Prior to the data synchronization, the backup application will prompt for confirmation:



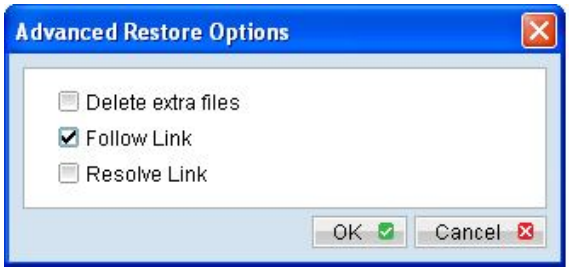
When using the [Delete extra files] option, please select the lowest possible child directories or files, instead of the highest parent directories for synchronization.

To demonstrate, assuming that you want to synchronize the restore destination (e.g. C:\Application) with the backed up C:\Application folder (restore source), select the Application folder, instead of the C:\ for restore.



8.1.4.1 Follow Link

Click on the [Advanced] button, select the [Follow Link] checkbox to enable the follow link option.



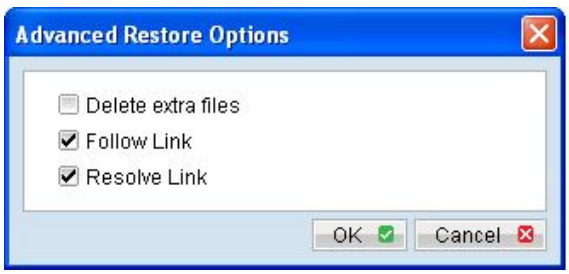
When the follow link option is enabled, not only is the symbolic link or junction point restored, and directories and files that the junction point links to will also be restored.

The following table summarizes the outcome when a restore is performed with different options.

Follow Link	Restore to	Action
Enabled	Original Location	Junction points are restored to the original location. Follow Link option enabled for backup - Target directories and files are restored to the original location. Follow link option disabled for backup - Target directories and files are not restored.
	Alternate Location	Junction points are restored to the location specified. Follow Link option enabled for backup - Target directories and files are restored to the location specified. Follow link option disabled for backup - Target directories and files are not restored.
Disabled	Original Location	Junction points are restored to the original location. No data is restored to the junction point's destination.
	Alternate Location	Junction points are restored to the location specified. No data is restored to the junction point's destination.

8.1.5.1 Resolve Link

Click on the [Advanced] button, select the [Resolve Link] checkbox to enable the resolve link option.



Note that the resolve link option is only available when the restore destination is configured to [Alternate location], and [Resolve Link] must be used in conjunction with the [Follow Link] option.

When the resolve link option is enabled, the junction point would be restored, and directories and files that the junction point links to will also be restored.

The following table summarizes the outcome when a restore is performed with different options.

Resolve Link	Action
Enabled	Junction points are restored to the alternate location specified, with its target directories and files also restored to the location specified in their relative path. Target of the junction is updated to the new relative path. In other words, junction now points to the new alternate location).
Disabled	Junction points are restored to the alternate location specified, with its target directories and files also restored to the location specified in their relative path. Target of the junction is not updated to the new relative path. In other words, junction now points to the original location.

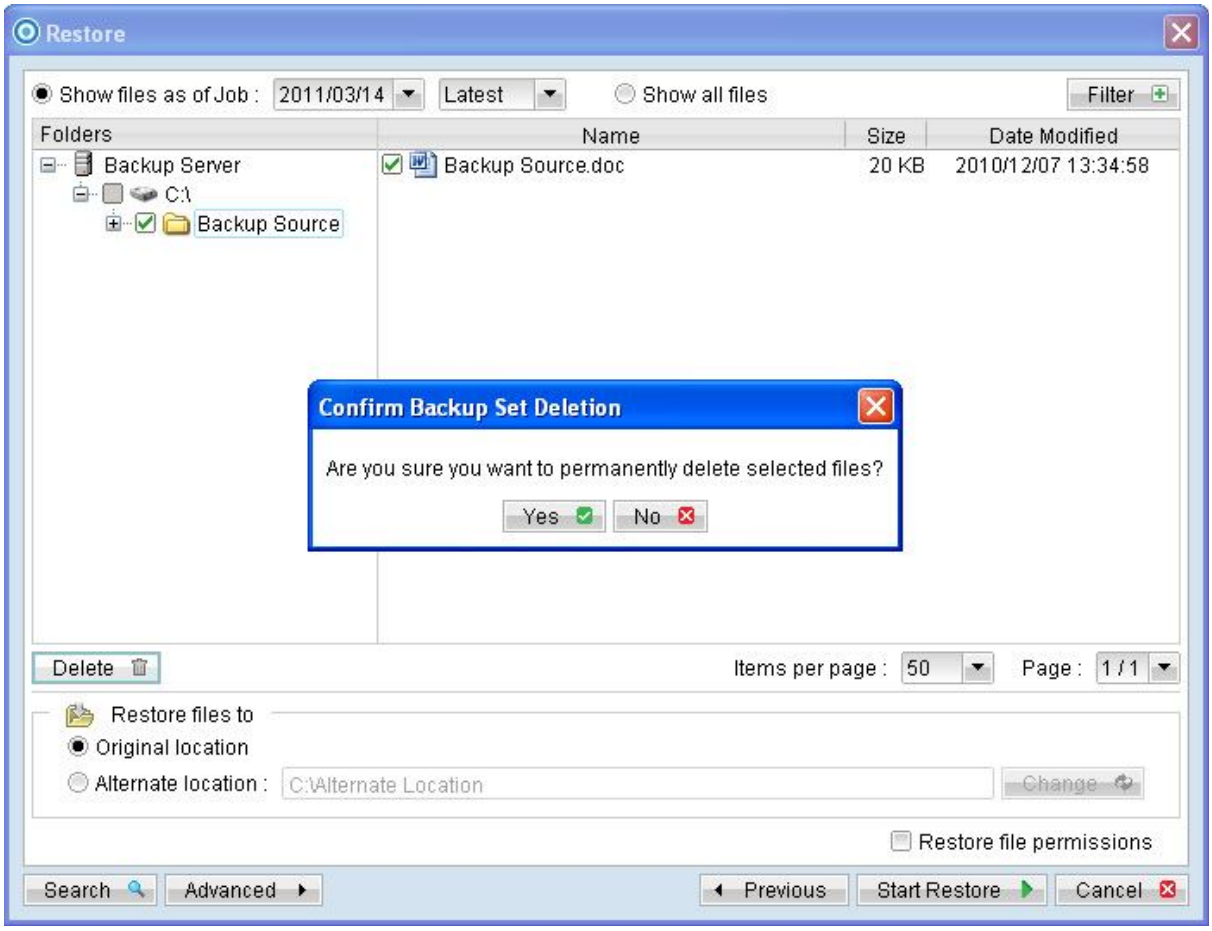
8.1.6.1 Delete backed up directories and files on backup server

Click on the [Delete] button to delete backed up data that reside on the backup server.

This option is useful for removing backed up directories or files on server that is no longer required.

Select the checkboxes beside the corresponding directories or files that you would like to delete, and click [Delete].

Prior to the data removal, the backup application will prompt for confirmation:



Important:
Files will no longer be available for restore after they are deleted from the backup server.

8.2 How to start a restore

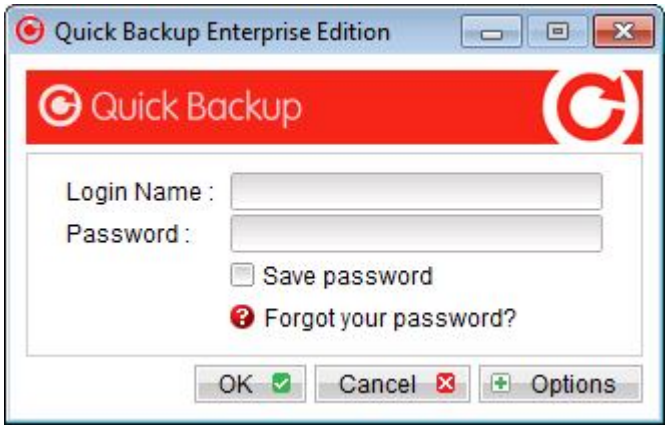
There are three methods for restoring data:

- Method 1 - Use of the backup client application user interface for restore on the client machine.
- Method 2 - Use of the web console interface for restore anywhere.
- Method 3 - Use of the Decrypt File Wizard for physical data copied from the backup server.

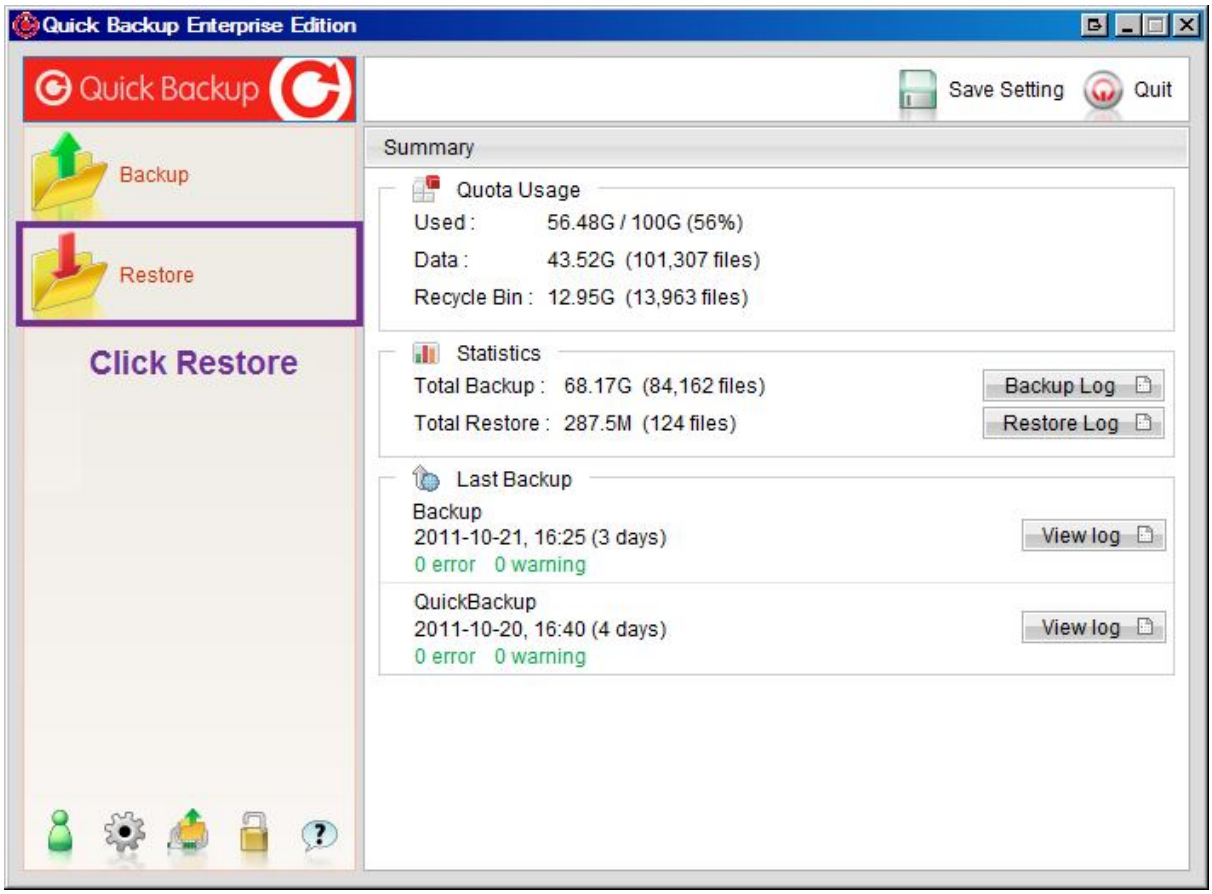
8.2.1 Restore using the Quick Backup user interface

Refer to the following steps for restore using the backup application's user interface:

1. Login to the backup application's user interface.



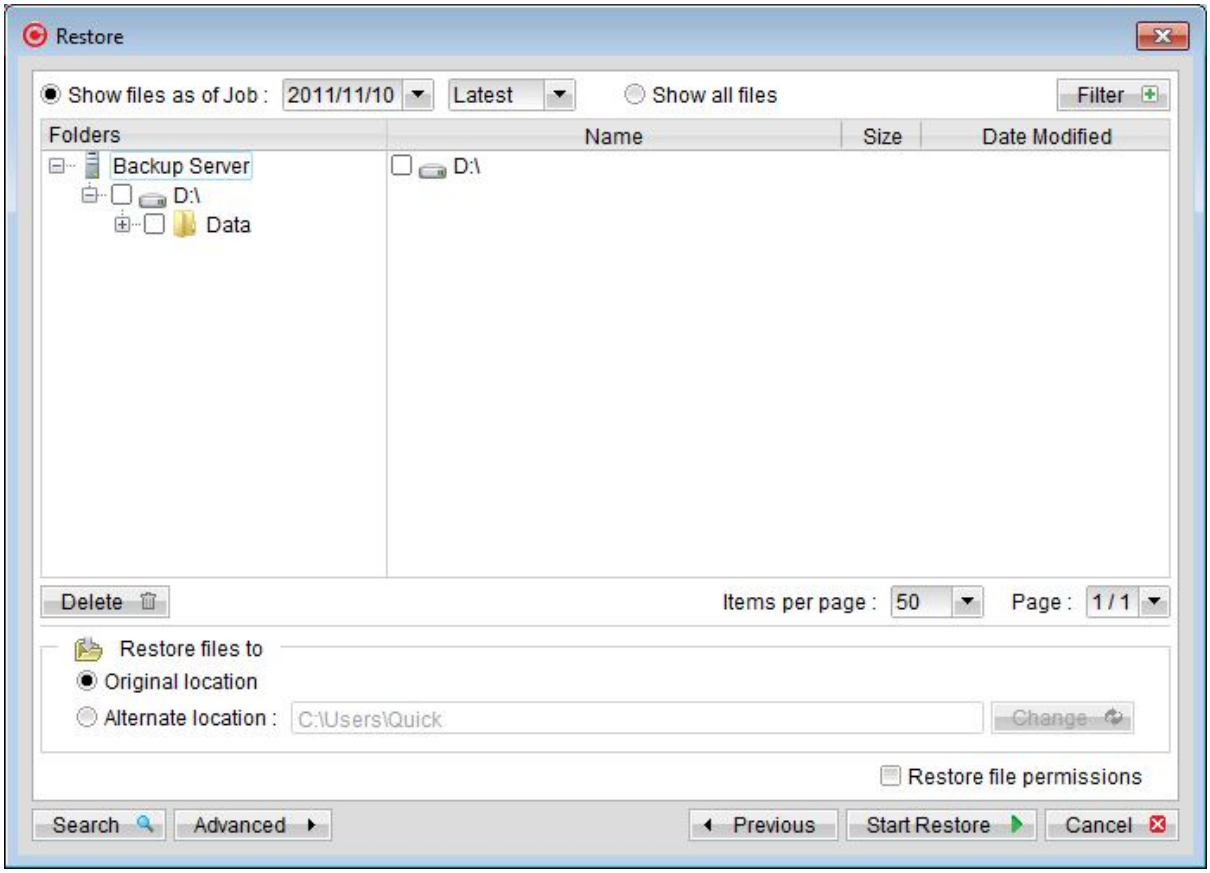
2. Click on the [Restore] button on the backup application's main window to open the Restore Menu.



3. Select the [Show files as of Job] to display files available as of a particular backup job.

For example, to display the files available for restore since the backup job performed on 11:00am Mar 11th, 2011. Select [Show files as of Job], [2011/03/11] and [11/00/00]

Select the [Show all files] to display all files available for restore.



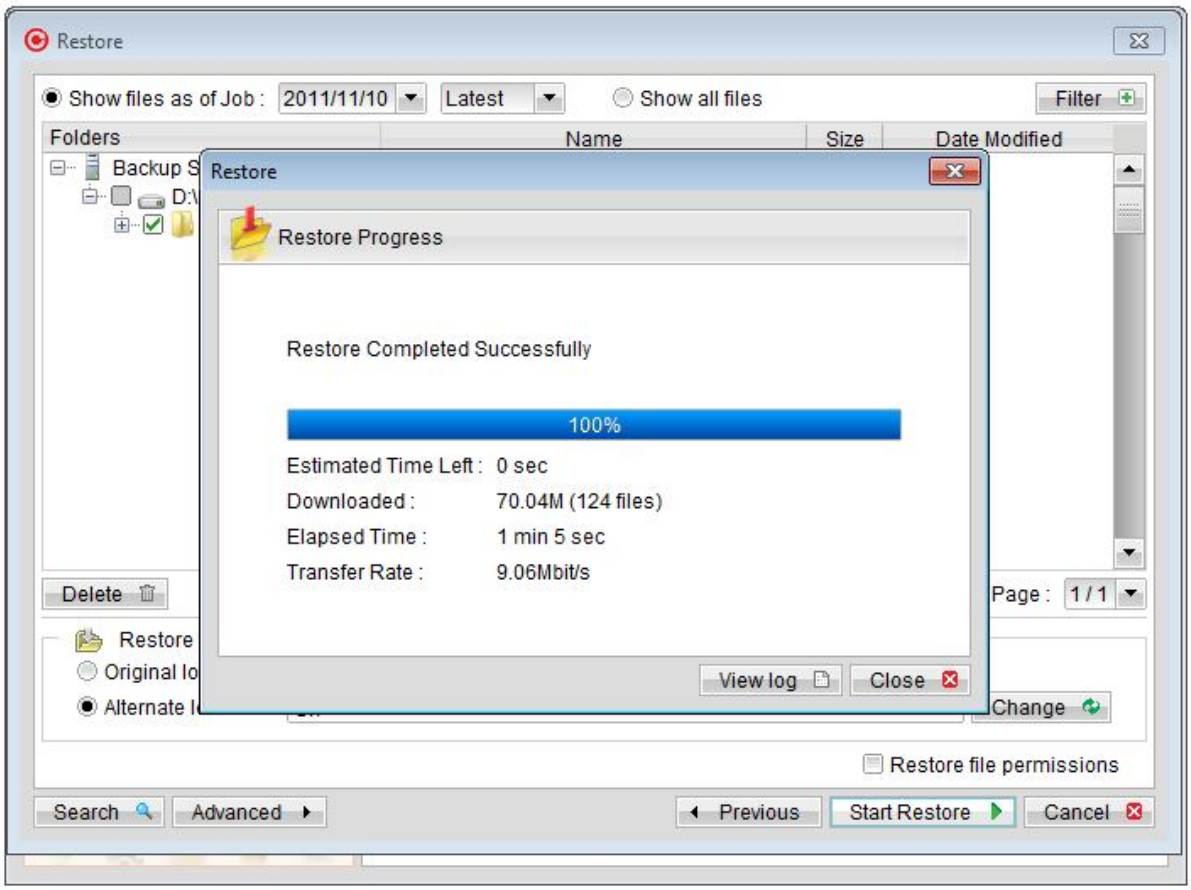
4. Expand the directories by selecting the ⊞ button beside a folder.

5. Make use of the other options such as [Filter], [Search] and [Advanced] option available, more details can be found in the sections above.

6. For restore to the original location on the client machine, select the [Original location] radio button.

   For restore to an alternate location, select the [Alternate location] radio button, and click [Change] to change the directory path which you would like to restore to.

7. Click [Start Restore] to begin the restore process.

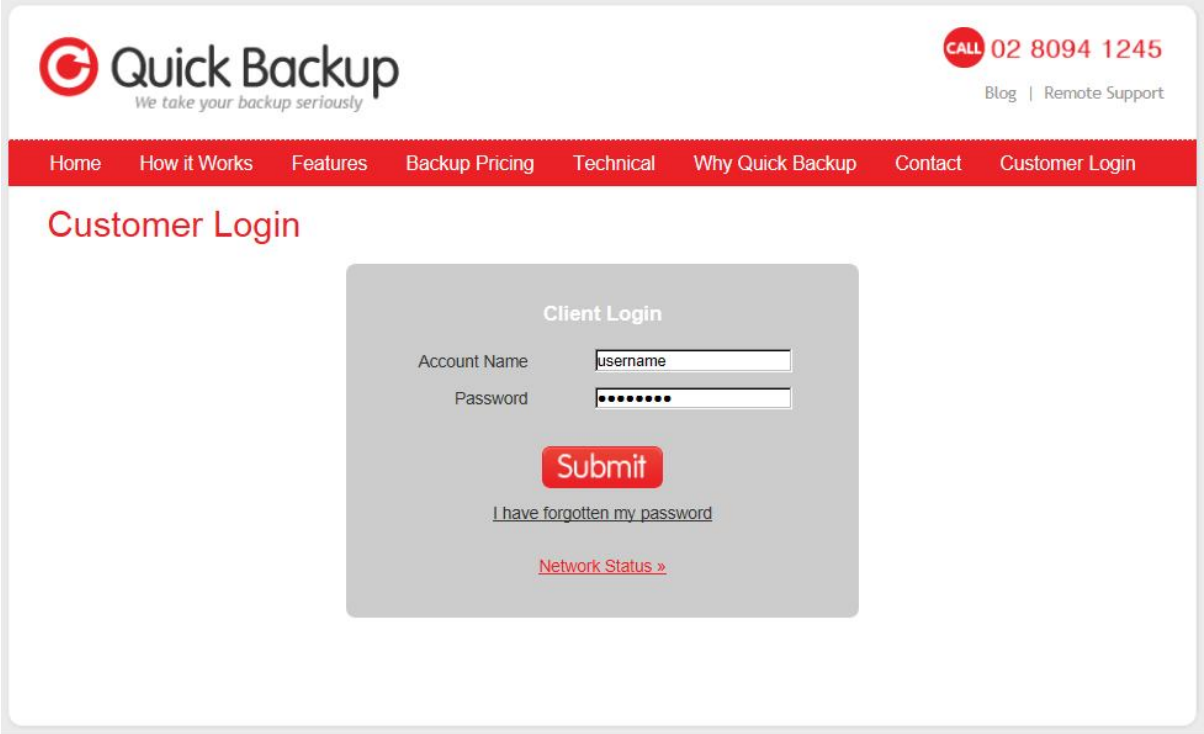

Restore
Show files as of Job :
2011/11/10
Latest
Show all files
Filter
Folders
Name
Size
Date Modified
Backup S
D:\
Restore
Restore Progress
Restore Completed Successfully
100%
Estimated Time Left : 0 sec
Downloaded : 70.04M (124 files)
Elapsed Time : 1 min 5 sec
Transfer Rate : 9.06Mbit/s
View log
Close
Delete
Page : 1 / 1
Restore
Original lo
Alternate l
Change
Restore file permissions
Search
Advanced
Previous
Start Restore
Cancel

8.2.2 Restore using the web interface

Refer to the following steps for restore using the web interface:

1. Login to the web interface at:

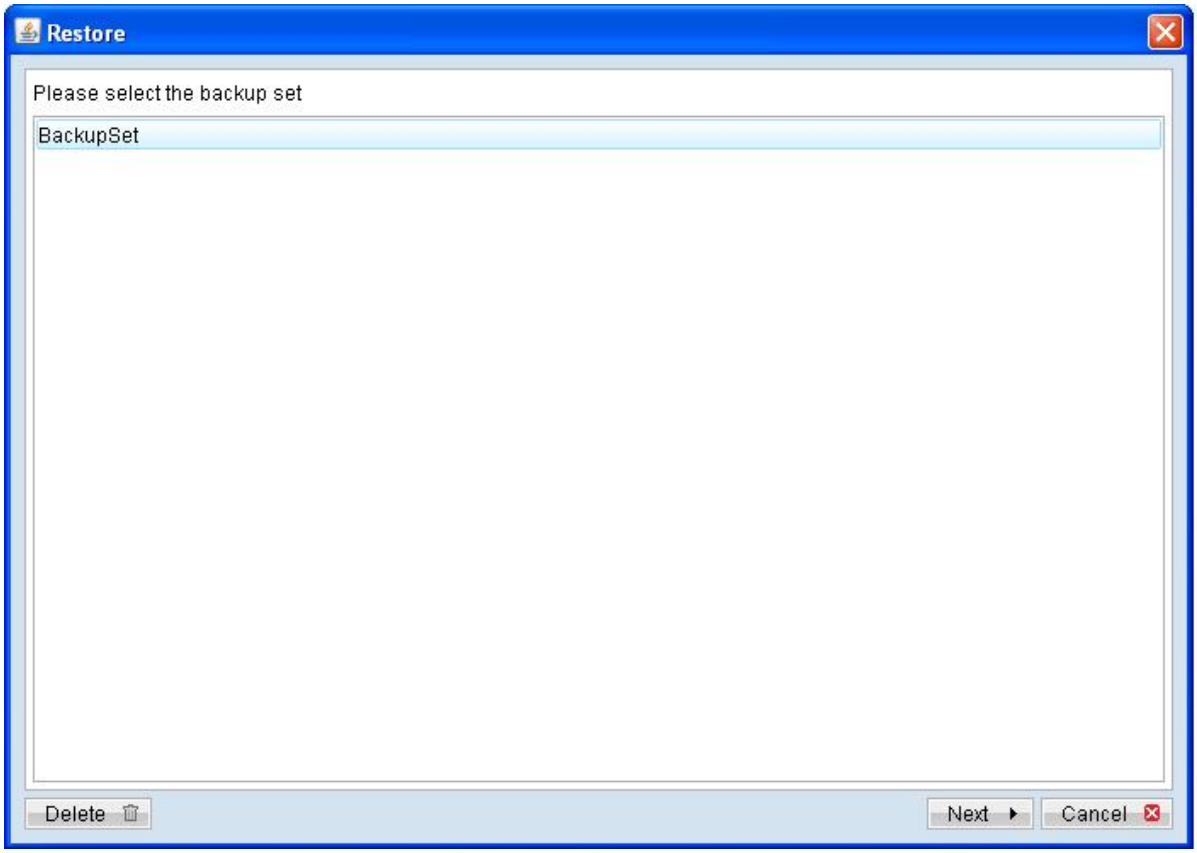
   https://www.quickbackup.com.au/customer-login



2. Click on the [File Explorer] tab at the top menu of the web interface.

Profile | Backup Set | File Explorer | Report | Statistics | Log
Logout
Home
Restore
Delete
Backup Set
Size
Last Modified
Zipped [Ratio]
BackupSet
Restore
Delete
Note:
1. This shows all backup sets available within this backup account.
2. To restore backup files, please click the [Restore] button shown above.
3. To delete a backup set, please click the [Delete] button shown above.

3. Click on the [Restore] button to open the web restorer applet:

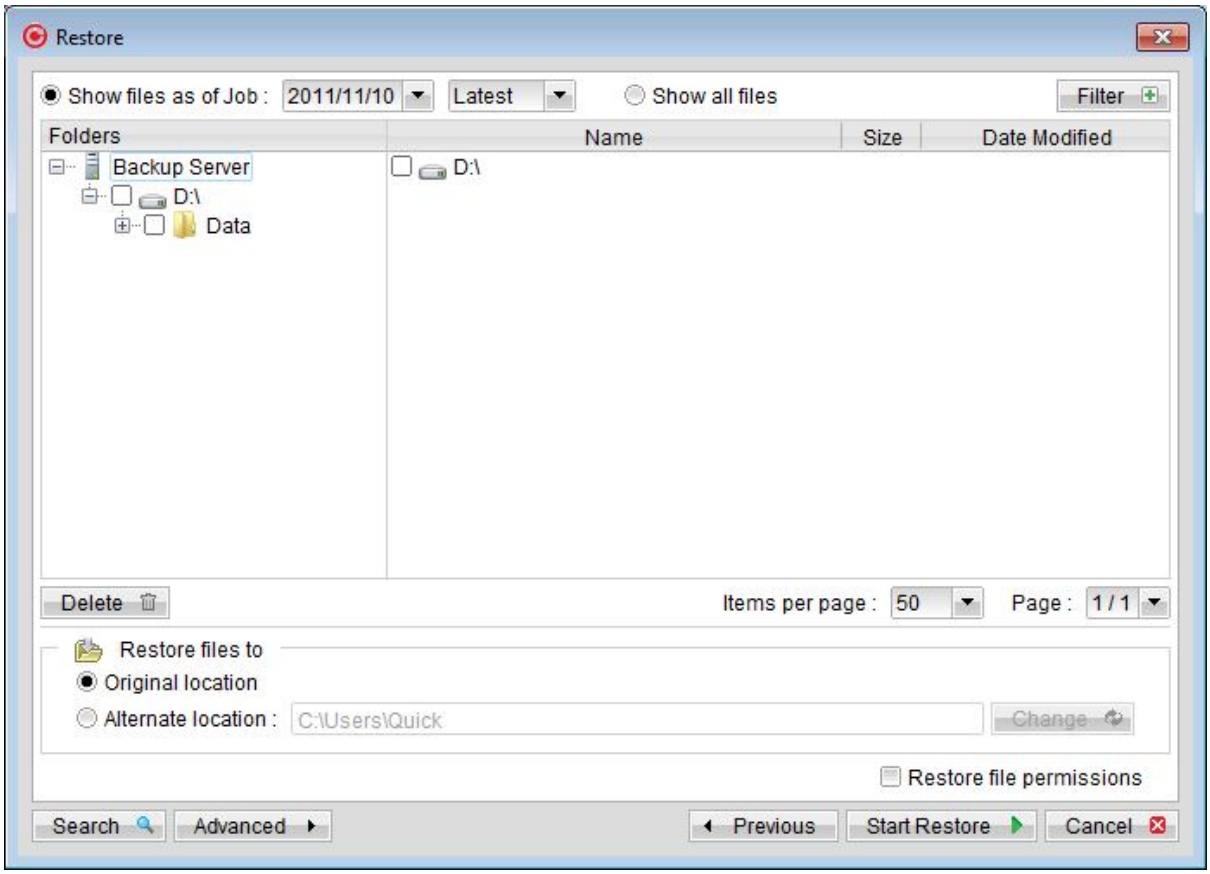


4. Select the corresponding backup set and press [Next]

5. Select the [Show files as of Job] to display files available as of a particular backup job.

   For example, to display the files available for restore since the backup job performed on 11:00am Mar 11th, 2011. Select [Show files as of Job], [2011/03/11] and [11/00/00]

   Select the [Show all files] to display all files available for restore.



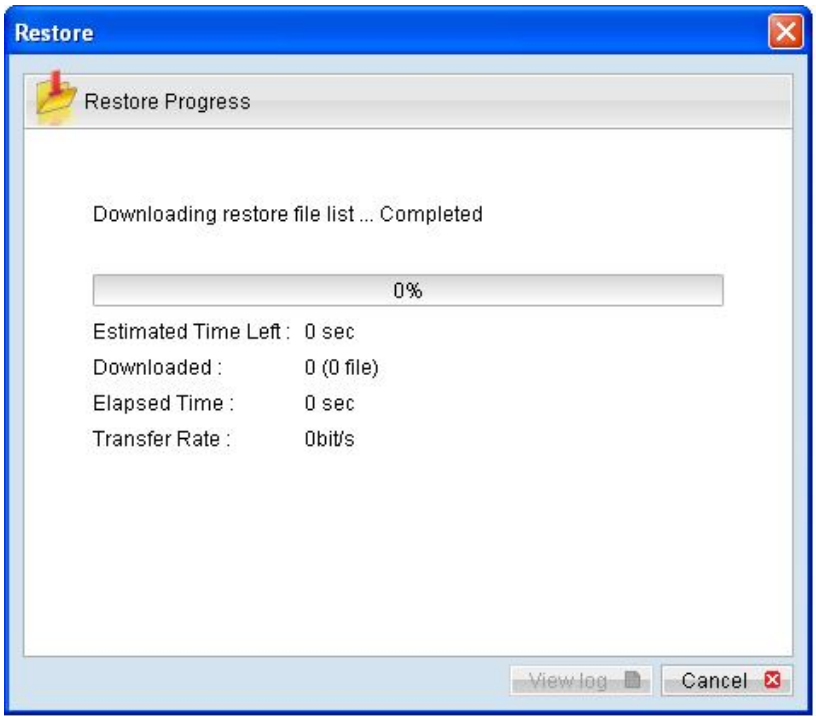
6. Expand the directories by selecting the ⊞ button beside a folder.

7. Make use of the other options such as [Filter], [Search] and [Advanced] option available, more details can be found in the earlier sections of this guide.

8. For restore to the original location on the client machine, select the [Original location] radio button.

   For restore to an alternate location, select the [Alternate location] radio button, and click [Change] to change the directory path which you would like to restore to.

9. Click [Start Restore] to begin the restore process.



8.2.3 Restore using Decrypt File Wizard

Data stored on the backup server can be copied onto a removable hard disk (or other storage medium) for direct restore on the client computer, bypassing the network bottleneck. This is especially useful for restore of large backup set.

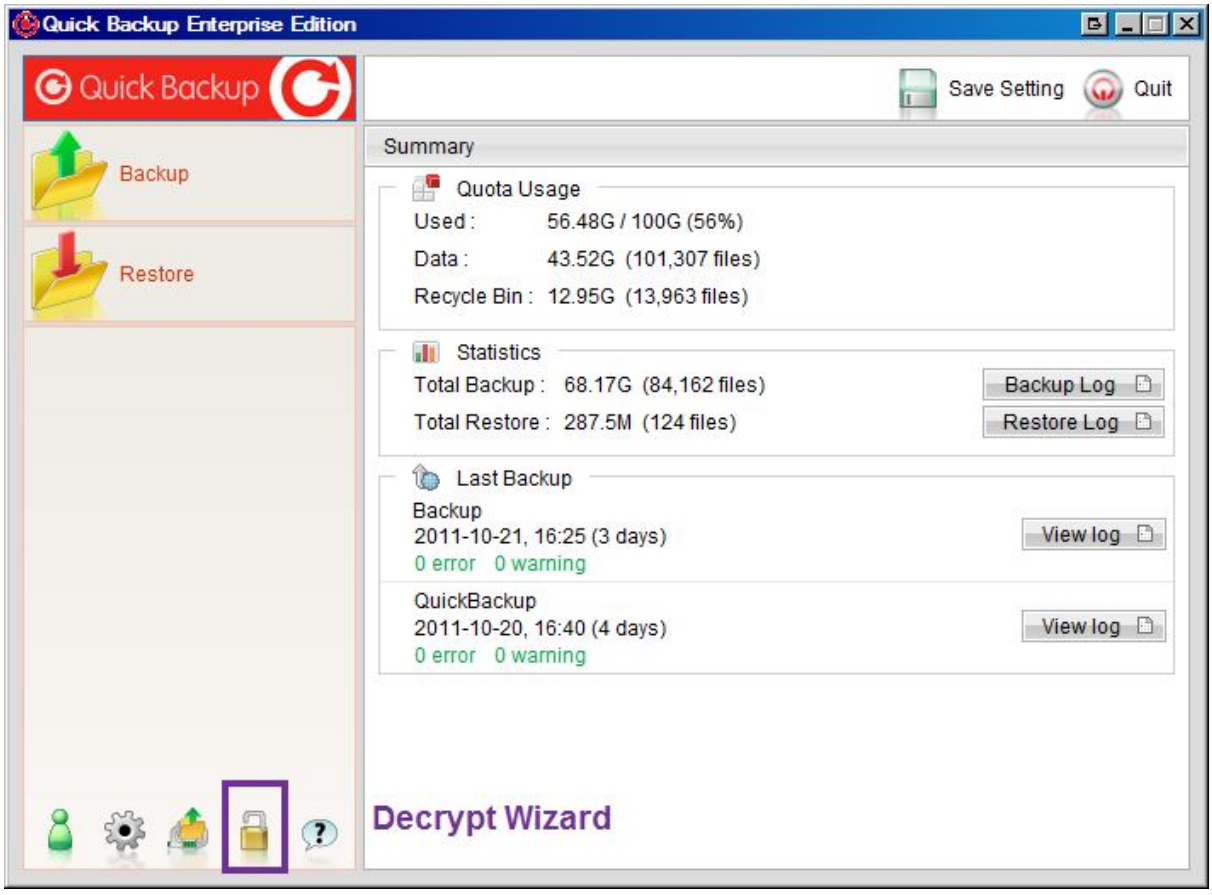
However, as data stored on the backup server are compressed and encrypted for security purposes, a utility called Decrypt File Wizard must be used to decrypt the data.

Refer to the following steps for restore using Decrypt File Wizard:

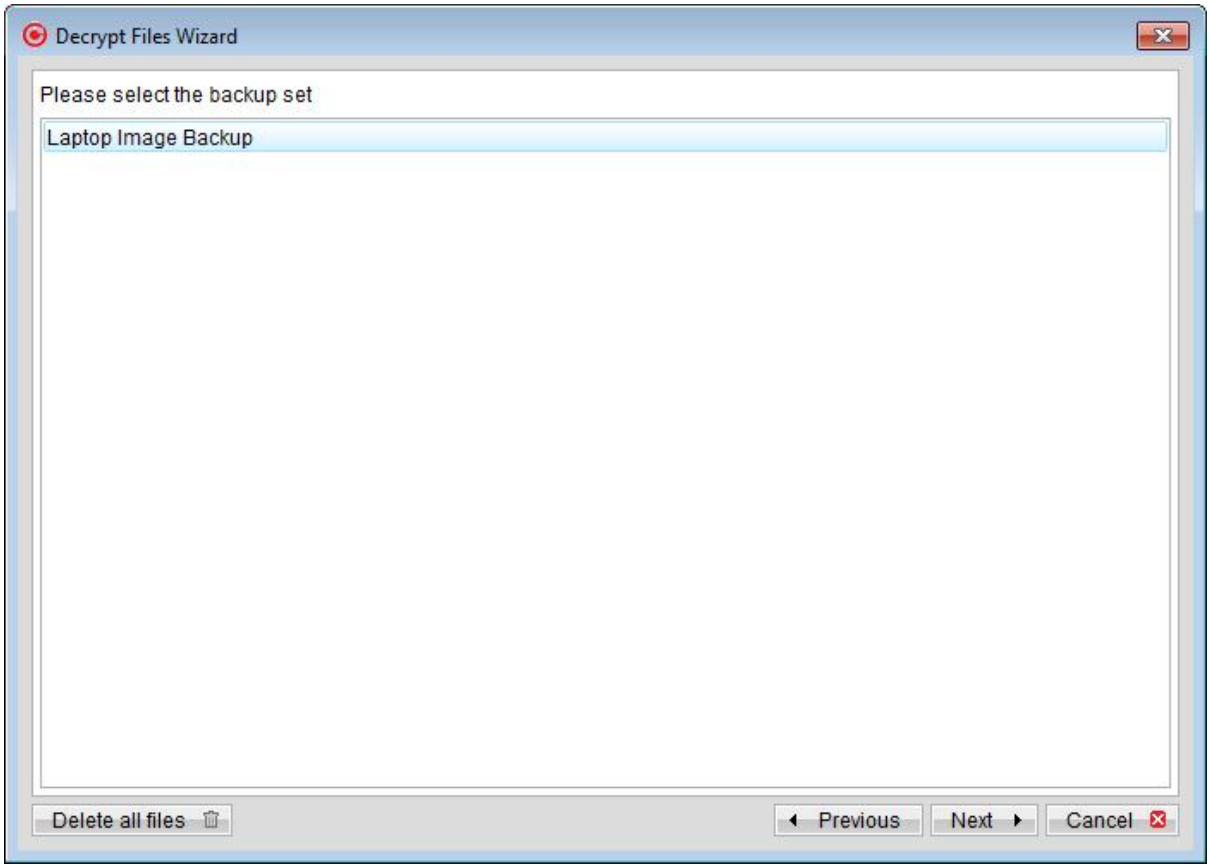
1. Connect the removable hard disk with the data to your computer.

2. Login to the backup application's user interface.

3. Click on the [Decrypt File Wizard] button on the backup application's main window to open the Decrypt File Wizard.



4. Select the [Change] button and browse to the [files] directory of the copied data, and click [Next].

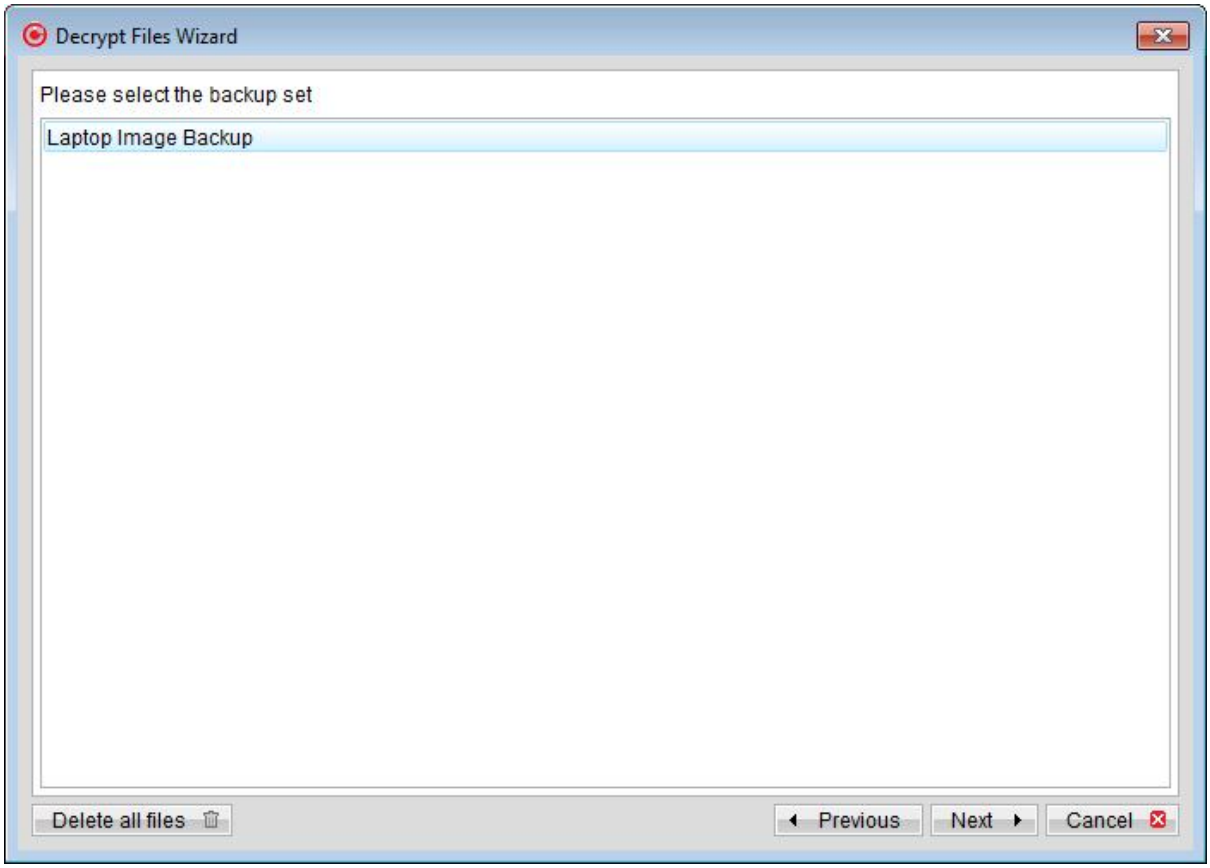


Note: Data copied onto the removable hard disk must be in the same directory structure as they are on the backup server, which is:

${Username}\files

Please contact your service provider if you cannot locate the [files] directory.

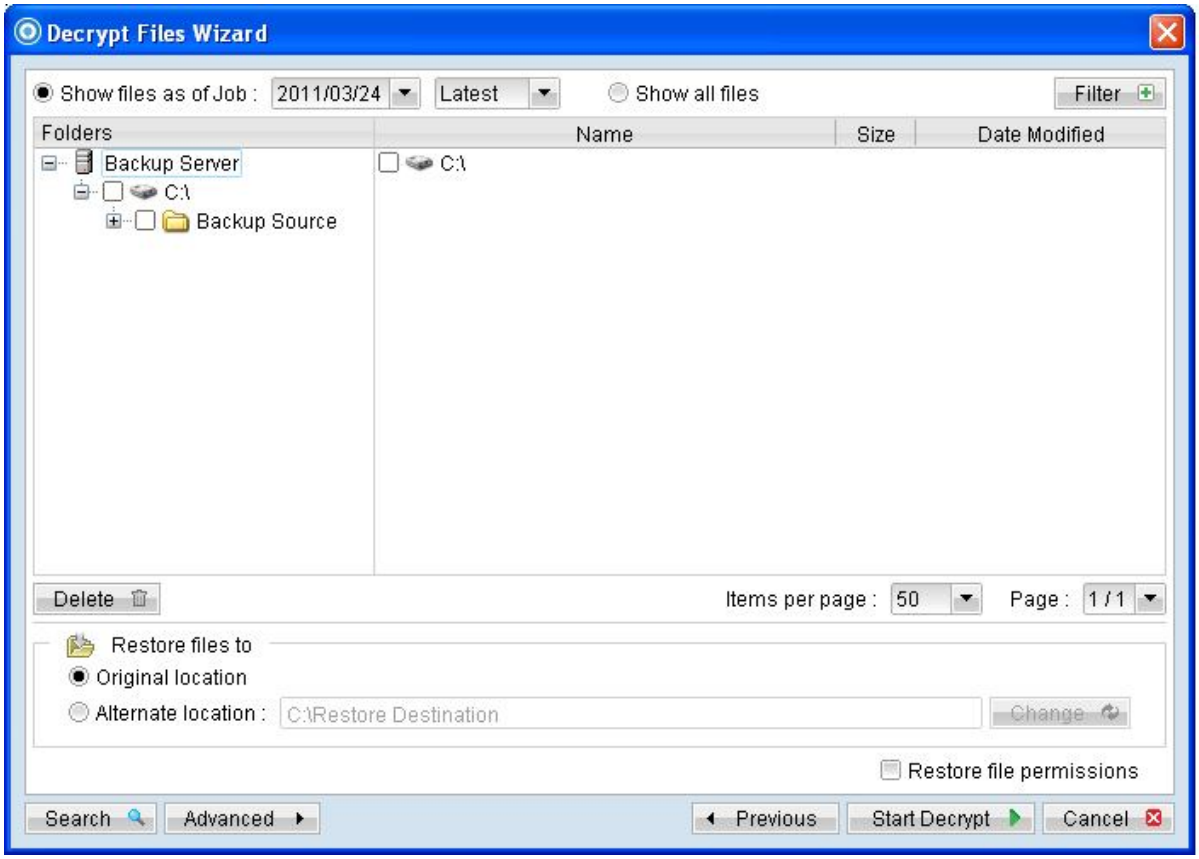
5. Select the corresponding backup set and press [Next]



6. Select the [Show files as of Job] to display files available as of a particular backup job.

   For example, to display the files available for restore since the backup job performed on 11:00am Mar 11th, 2011. Select [Show files as of Job], [2011/03/11] and [11/00/00]

   Select the [Show all files] to display all files available for restore.



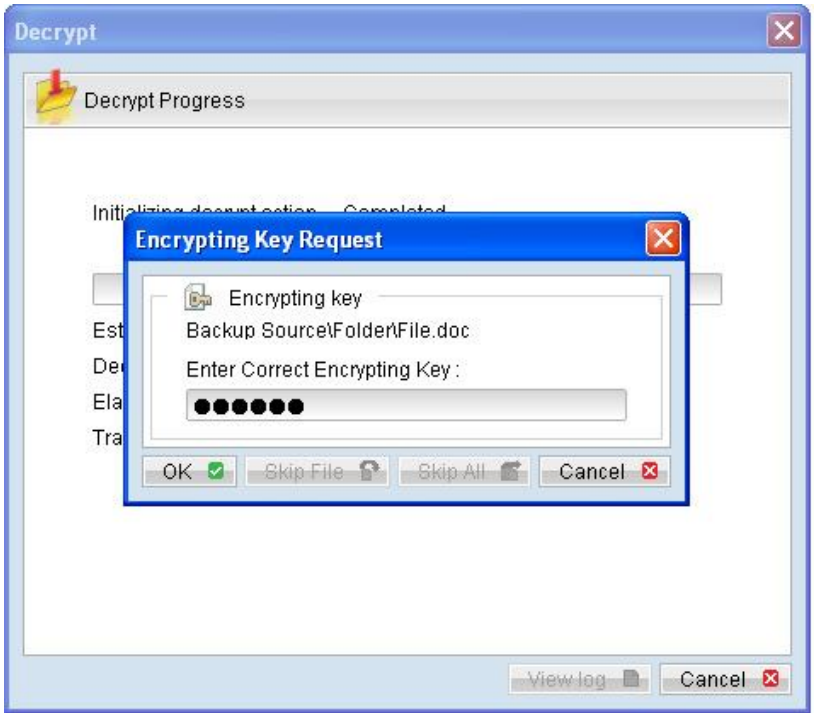
7. Expand the directories by selecting the ⊞ button beside a folder.

8. Make use of the other options such as [Filter], [Search] and [Advanced] option available, more details can be found in the sections above.

9. For decrypt to the original location on the client machine, select the [Original location] radio button.

   For decrypt to an alternate location, select the [Alternate location] radio button, and click [Change] to change the directory path which you would like to restore to.

10. Click [Start Decrypt] to begin the decrypt process.



8.3 IP restriction for restore using the web interface

IP address restriction can be imposed on the backup server to restrict computer with un-authorized IP address from restoring data using the web interface.

Please contact Quick Backup for more information on this option.

9 In-file Delta Technology

This chapter describes what In-file delta technology is and how it can be used to reduce size of backup.

9.1 Overview

In-file delta technology is an advanced data block matching algorithm with the intelligence to pick up changes (delta) of file content between two files.

Using this algorithm, daily backup of large files over low-speed internet connection is made possible because it requires only the changes of information since the last backup to be sent over (assuming that the full backup of the file has been saved on the backup server already).

This is what will happen in the backup of a 10 GB Outlook.pst file when it is backed up by Quick Backup with In-file delta technology:

1. The whole file (10 GB) with its checksum file, are backed up to the backup server. This can be done directly through the internet or indirectly using the seed loading utility

2. When the backup runs again later (sub-sequence backup), Quick Backup will download a checksum listing of all data blocks of the full backup file (or last incremental backup file) from the backup server and use it to pick up all changes that have been made to the current Outlook.pst file.

3. Changes detected are then saved in a delta file which is uploaded to the backup server. A new checksum file is generated and is also uploaded. (This delta file is assumed to be small because the content of PST files doesn't change a lot during daily usage).

4. Sub-sequent backups of this 10 GB Outlook.pst file will go through step 2 and step 3 again. As explained, only a small delta file and checksum file will be uploaded to the backup server.

5. With In-file delta technology, daily backing up of large file over low-speed internet connection is now possible.

Incremental In-file delta
Incremental Delta will facilitate ease of backup.

The delta is generated by comparing with the last uploaded full or delta file. Delta generated with this method is smaller and uses the least bandwidth.

However, for restoration, the full file and all deltas up to the required point-in-time are required to be restored and merged.

For example:
This is what will happen in the backup of a 10 GB Outlook.pst file with 100 MB increment each day.

After the initial full backup, the backup application would continue to generate and upload delta instead of the full file until one of the following two rules are true:

- Number of delta files generated (since the last full backup) exceeded the [No. of Delta] setting.

- The delta ratio (ratio of delta file size against the full file size) exceeded the [Delta Ratio] setting.

With incremental delta, delta generated by comparing the current file with the last uploaded file (full or delta) is around 100 MB.

Since the delta file size is about 100 MB daily, delta ratio of 1% would not trigger a full file upload.

Instead, Quick Backup will continue to generate and upload delta files until day 102 (full file uploaded on day 1) when the number of deltas generated exceeds the [No. of Delta] setting.

All delta files are generated with respect to changes made since the last incremental or full backup. This means that the last full backup file and ALL incremental delta backup files are required to restore the latest snapshot of a backup file.

Differential In-file delta
Differential Delta will facilitate ease of restore.

The delta is generated by comparing with the last uploaded full file only. Delta generated with this method will grow daily and uses more bandwidth.

However, for restoration, the full file and a single delta is required to be restored and merged.

For example:
This is what will happen in the backup of a 10 GB Outlook.pst file with 100 MB increment each day.

After the initial full backup, the backup application would continue to generate and upload delta instead of the full file until one of the following two rules are true:

- Number of delta files generated (since the last full backup) exceeded the [No. of Delta] setting.

- The delta ratio (ratio of delta file size against the full file size) exceeded the [Delta Ratio] setting.

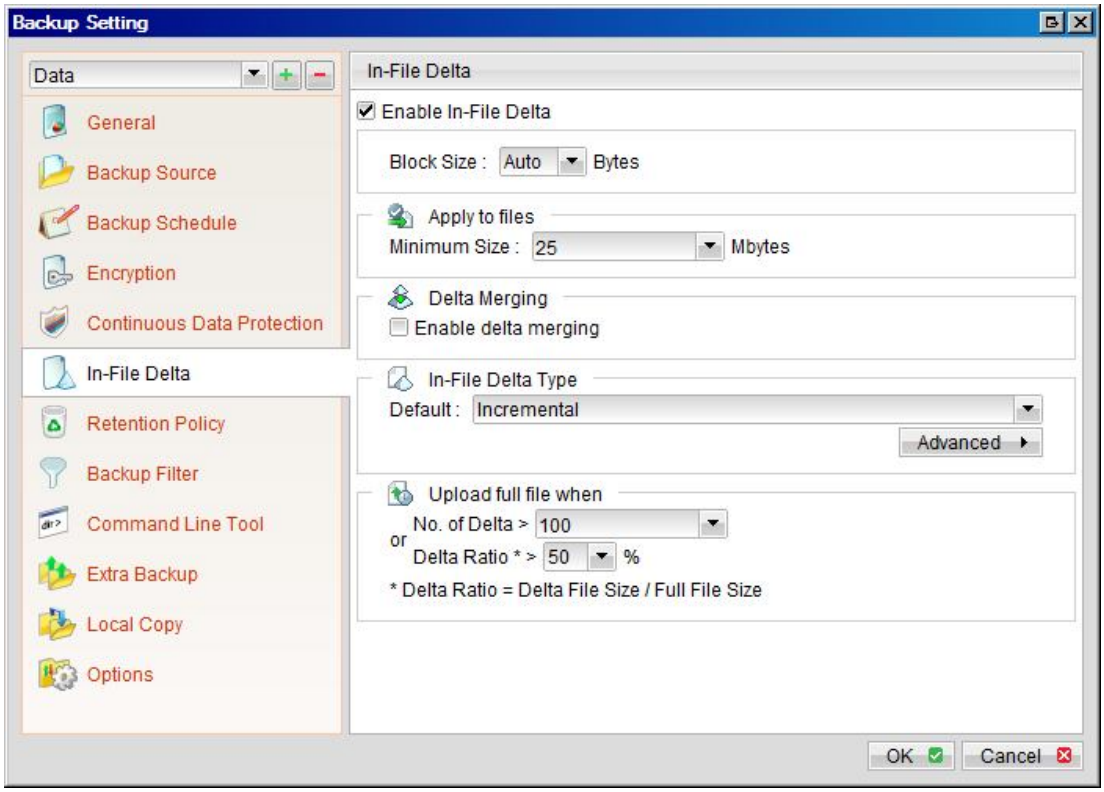
With differential delta, delta generated by comparing the current file with the last full file is about 100 MB for the 1st delta, 200 MB for the 2nd delta, and 300 MB for the 3rd delta (increment of 100 MB per day).

Since the delta file size increase by 100 MB per day, Quick Backup will continue to generate and upload delta files until day 52 (full file uploaded on day 1) when the delta ratio exceeds the [Delta Ratio] setting:

Delta file size of approximately 51 × 100 MB = 5.1 GB.

All delta files are generated with respect to changes made since the last full backup. This means that only the last full backup file and the last delta file are required to restore the latest snapshot of a backup file.

*In the event of corrupted delta file, only one particular snapshot of the file is non-restorable. All other snapshots with its delta would remain intact.



9.1.1 Block Size

[Block Size] defines the size of block used when detecting changes between last full or delta file and the file to be backed up.

In general:

In-file delta backup with small block size:

- Produce a smaller delta file due to a more precise comparison
- Require more processing power on the client machine
- Comparison may take longer to complete

In-file delta backup with large block size:

- Produce a larger delta file due to a less precise comparison
- Require less processing power on the client machine
- Comparison will complete faster

For most cases, the default setting [Auto] will select the optimal block size for each file (depending on the size of the file).

9.1.2 Apply to files (Minimum Size)

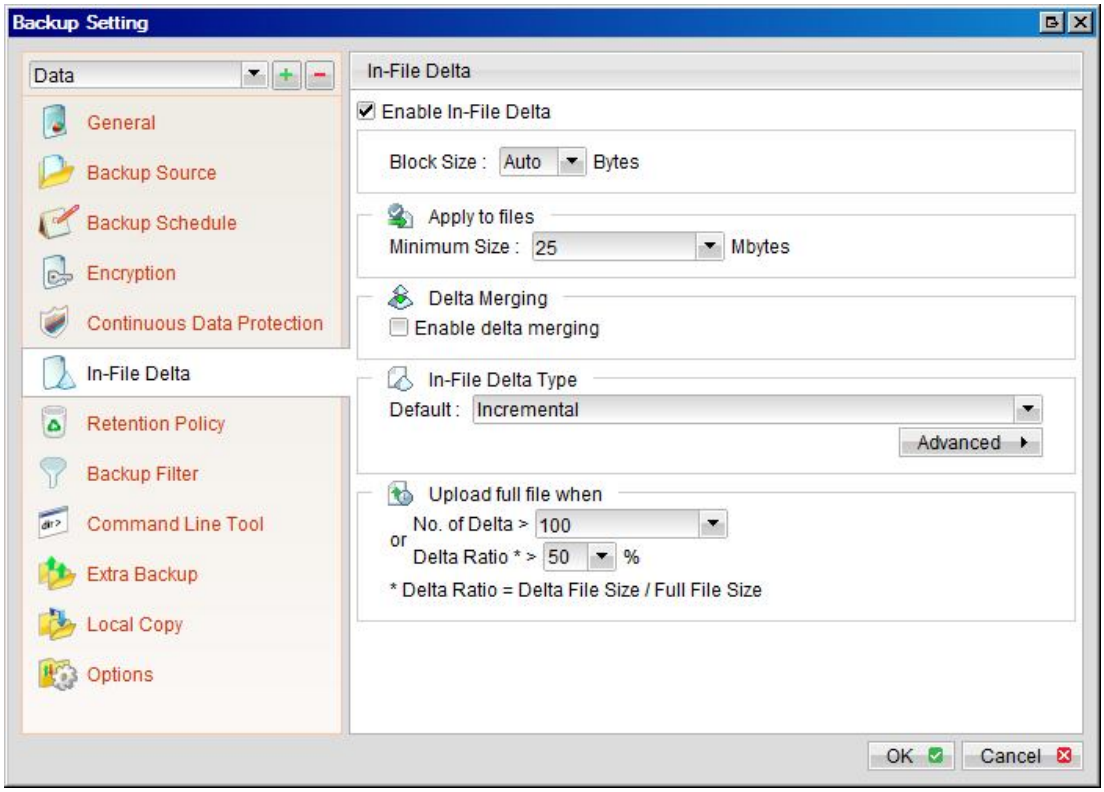
[Apply to files (Minimum Size)] defines the smallest file size a file must have before the use and application of In-file delta technology.

If the size of a file that is being backed up is smaller than the [Minimum File Size] setting, In-file delta technology will not be applied to this file and the whole file will be uploaded to the backup server.

It is not necessary to perform In-file delta backup on small files because backing up the whole file does not take long. Backing up the whole file instead reduces the time required to restore the file..

9.1.3 Delta Merging (Enable delta merging)

[Delta Merging (Enable delta merging)] defines whether to enable the delta merge feature for the corresponding backup set.



To enable the delta merging feature, select the [In-File Delta] tab in the [Backup Setting] menu, and select the checkbox beside [Enable delta merging].

9.1.1.3 Overview

The delta merge feature combines the full and delta files (differential or incremental) on Quick Backup Server into a single full file.

The advantage of using delta merge is it will speed up the restore of files. As a single 'merged' file can be restored faster than a file consisting of full plus related incremental files, which may require a lengthy merging process after restoring to a client machine.

Delta merge can be applied to full and differential or incremental delta files which reside in the data area. The criteria for file merging are governed by the retention policy setting for the backup set.

9.1.2.3 Limitation

The following are limitations of the delta merge feature:

- Delta merge cannot be performed for abnormal backup set with multiple encryption key
- Advanced retention policy cannot be used in conjunction with the delta merge feature.

- The delta merge of differential delta files with the full file, will only apply if there are incremental delta files present in the delta chain. Therefore, no delta merge will take place for backup sets with delta merge enabled and in-file delta set to Differential.

- The delta merge feature does not support Local Copy backup.

9.1.3.3 Delta Merge Policy

The delta merge process relies on the retention policy setting to decide when to merge delta files with the full file. But delta merge does not apply to files in the retention area. Any backup sets configured with advanced or customized retention policy settings cannot use the delta merge feature.

Any reference to retention policy in the context of delta merge implies delta merge policy. As backup sets enabled with delta merge share a single setting, any changes in retention policy will impact on the availability of snapshots that can be restored from both data and retention area. Before enabling the delta merge feature please review your data restore requirements carefully

9.1.4.3 Delta Merging Process

A delta merge will take place after a backup job is completed, Quick Backup will only initiate a delta merge request at the end of a backup job.

As part of the request, Quick Backup will upload a copy of the backup set encryption key to Quick Backup Server which is hashed for security purposes. Once a merge request is received by Quick Backup Server it will be placed in the delta merge queue, the information in the delta merge queue only exists in memory for security purposes.

Delta merge of a file can only be run once every 24 hours.

The 24 hour period is calculated from the start time of the previous delta merge and the start time of the current merge.

As backup sets enabled with delta merge share a single setting, any changes in retention policy will impact on the availability of snapshots that can be restored from both data and retention area.

Important:
Before enabling the delta merge feature please review your data restore requirements carefully.

9.1.5.3 Delta Merging Example

The following is some simple examples to demonstrate the functionality of the delta merge feature:

Example 1:

The example below shows how delta files are merged into full file using a retention policy (delta merge policy) setting defined as 4 jobs for this backup set.

A full backup file is stored into data area (F) uploaded by Job 1, followed by incremental delta files I_1, I_2, I_3, and I_4. On the completion Job 5 (I_4), the backup application will trigger a delta merge background job to execute the file merging. When the Quick Backup Server delta merge job runs F + I_1 will be merged to become a merged full file. The data area now contains 4 snapshots including merged full file after file merging.

Retention Policy = 4 Jobs (Delta Merge Policy)

Job 1 = F
Job 2 = I_1
Job 3 = I_2
Job 4 = I_3
Job 5 = I_4 (delta merge initiated)

After job 5 the backup application will initiate a delta merge for Job 1 & Job 2 files.

F (F + I_1) merged full file
I_2
I_3
I_4

Example 2:
The example below shows how delta files are merged into full file using a retention policy (delta merge policy) setting defined as 7 days for this backup set.

A full backup file is stored into data area (F) uploaded on Day 1, followed by incremental delta files I_1, I_2, I_3, I_4, I_5, I_6, I_7, and I_8,. On the completion of the backup job on Day 9 (I_8), the backup application will trigger a delta merge background job to execute the file merging. When the Quick Backup Server delta merge job runs F + I_1 will be merged to become a merged full file. The data area now contains 8 snapshots including merged full file after file merging.

Retention Policy = 7 Days (Delta Merge Policy):

Day 1 = F
Day 2 = I_1
Day 3 = I_2
Day 4 = I_3
Day 5 = I_4
Day 6 = I_5
Day 7 = I_6
Day 8 = I_7
Day 9 = I_8 (delta merge initiated)

After job on day 9 the backup application will initiate a delta merge for Day 1 & Day 2 files. As the incremental file I_1 has exceeded the 7 day retention policy setting.

F (F + I_1) merged full file
I_2
I_3
I_4

I_5
I_6
I_7
I_8

Example 3:
This example below shows what happens when there are multiple backup jobs occurring which generates incremental delta files within a 24 hour period.

A full backup file is stored into data area (F) uploaded by Job 1, followed by incremental delta files I_1, I_2, I_3, and I_4. On the completion Job 5 (I_4), the backup application will trigger a delta merge background job to execute the file merging. When the Quick Backup Server delta merge job runs F + I_1 will be merged to become a merged full file.

Retention Policy = 4 Jobs (Delta Merge Policy)

Job 1 = F
Job 2 = I_1
Job 3 = I_2
Job 4 = I_3
Job 5 = I_4 (delta merge initiated)
Job 6 = I_5
Job 7 = I_6

After job 5 the backup application will initiate a delta merge for Job 1 & Job 2 files. If after the delta merge there are further incremental uploads, i.e. Job 6 and Job 7. These increment files will not be merged by Quick Backup Server as a delta merge jobs has already taken place within the last 24 hours. The data area now contains 6 jobs, which exceeds the delta merge policy of 4 jobs

F (F + I_1) merged full file
I_2
I_3
I_4
I_5
I_6

Quick Backup Server will merge the extra incremental files, when the next backup job completes 24 hours after the last delta merge. Quick Backup Server will merge all the delta files which have exceeded the backup set delta merge policy.

Example 4:
The example below shows how differential and incremental delta files are merged into full file using a retention policy (delta merge policy) setting defined as 4 jobs for this backup set.

A full backup file is stored into data area (F) uploaded by Job 1, followed by incremental and differential delta files I_1, I_2 I_3 and D_1.

Retention Policy = 4 Jobs (Delta Merge Policy)

Job 1 = F
Job 2 = I_1

Job 3 = I_2
Job 4 = I_3
Job 5 = D_1 (delta merge initiated)

After Job 5 the backup application will initiate a delta merge for Job 1 & Job 2. Unfortunately, differential delta D_1 is found in delta chain, this creates delta merge stoppage, the files in Job 1 and Job 2 will not be merged.

The backup job continues with subsequent incremental backups (I_4, I_5 and I_6).

Job 1 = F
Job 2 = I_1
Job 3 = I_2
Job 4 = I_3
Job 5 = D_1 (delta merge is initiated and stopped)
Job 6 = I_4 (delta merge is initiated and stopped)
Job 7 = I_5 (delta merge is initiated and stopped)
Job 8 = I_6 (delta merge is initiated)

After Job 8 the backup application will initiate a delta merge, Quick Backup Server will merge the full file (F) uploaded in Job 1 with the differential delta D_1 uploaded in Job 5 to form the new full file (As the D_1 differential includes changes in $I_1 + I_2 + I_3$). The incremental files $I_1 + I_2 + I_3$ will be moved to the retention area, as they have already exceeded the retention policy of 4 jobs. These files will be purged on the next retention policy job.

After the delta merge has completed the follow files will be available for restore.

F ($F + D_1$)
I_4
I_5
I_6

Example 5:
The example below shows how delta merge handles multiple differential delta files using a retention policy (delta merge policy) setting defined as 4 jobs for this backup set.

A full backup file is stored into data area (F) uploaded by Job 1, followed by incremental and differential delta files I_1, I_2 I_3 and D_1.
Retention Policy = 4 Jobs (Delta Merge Policy)

Job 1 = F
Job 2 = I_1
Job 3 = I_2
Job 4 = I_3
Job 5 = D_1 (delta merge initiated)

After Job 5 the backup application will initiate a delta merge for Job 1 & Job 2. Unfortunately, differential delta D_1 is found in delta chain, this creates delta merge stoppage, the files in Job 1 and Job 2 will not be merged.

The backup job continues with subsequent differential delta backups (D_2 and D_3) and incremental delta backups (I_4, I_5, and I_6).

Job 1 = F
Job 2 = I_1
Job 3 = I_2
Job 4 = I_3
Job 5 = D_1 (delta merge is initiated and stopped)
Job 6 = D_2 (delta merge is initiated and stopped)
Job 7 = D_3 (delta merge is initiated and stopped)
Job 8 = I_4 (delta merge is initiated and stopped)
Job 9 = I_5 (delta merge is initiated and stopped)
Job 10 = I_6 (delta merge is initiated)

After Job 10 the backup application will initiate a delta merge, Quick Backup Server will merge the full file (F) uploaded in Job 1 with the latest differential delta D_3 uploaded in Job 7 to form the new full file (As the D_3 differential includes changes in $I_1 + I_2 + I_3 + D_1 + D_2$). The files $I_1 + I_2 + I_3 + D_1 + D_2$ will be moved to the retention area, as they have already exceeded the retention policy of 4 jobs. These files will be purged on the next retention policy job.

After the delta merge has completed the follow files will be available for restore.

F ($F + D_3$)
I_4
I_5
I_6

9.1.4 In-File Delta Type

The [In-file Delta Type] setting defines the way In-File Delta files are handled. There are two different versions as follows:

Incremental In-File Delta
All delta files are generated with respect to changes made since the last incremental backup. This means that the last full backup file and all related incremental delta backup files are required to restore the latest snapshot of a backup file.

The full backup file, its checksum file and all incremental delta files are always stored in the data area. This means that these files are not affected by the setting of the retention policy and will always be kept on the backup server. However, for backup sets with delta merge enabled, the retention policy setting is also used by the delta merge feature to determine when Quick Backup Server will merge the full and incremental delta files into a new full file.

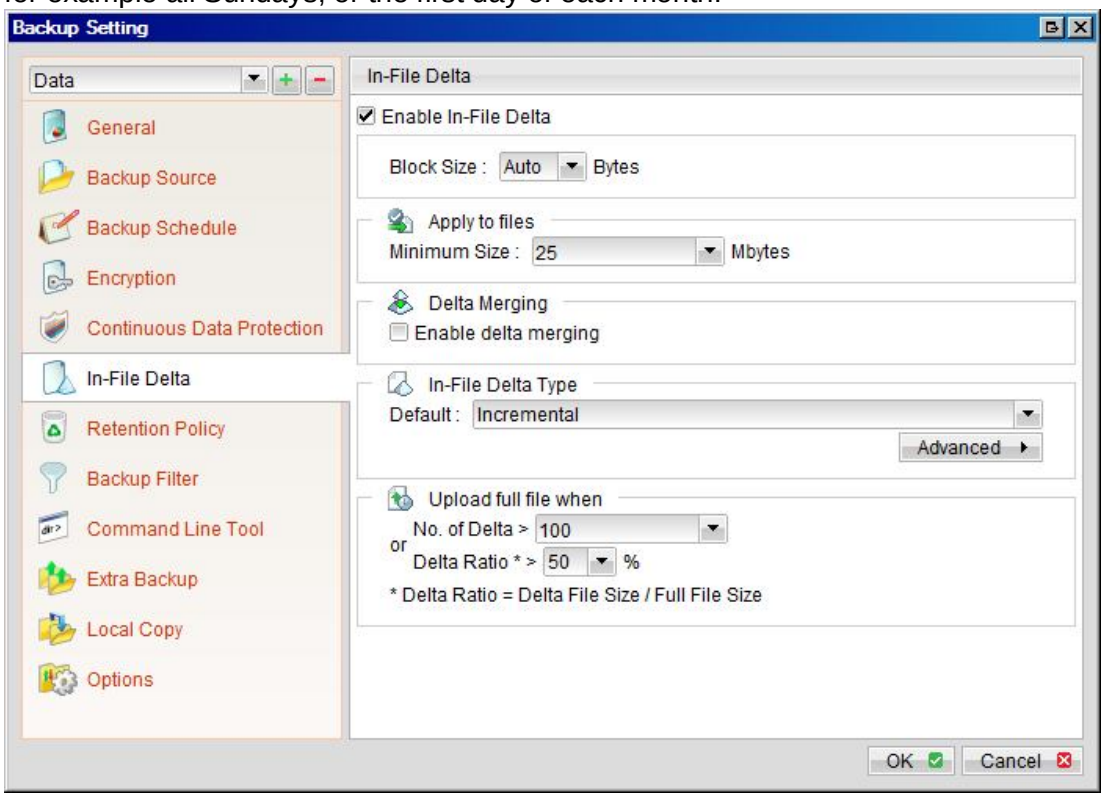
Differential In-File Delta
All differential delta files are generated with respect to changes made since the last full backup file. This means that only the last full backup file and the last differential delta file are required to restore the latest snapshot of a backup file. The other intermediate differential delta files are only required if you want to restore intermediate snapshots of a backup file.

The advantage of a differential In-File delta backup is that a corrupted differential delta file would only make one particular snapshot of a backup file non-recoverable. All other snapshots can still be recovered using the remaining differential delta files.

The full backup file, its checksum file and the last delta file uploaded (if more than one delta files have been uploaded to the backup server) is always stored in the data area. This means that these files are not affected by the setting of the retention policy and will always be kept on the backup server. It is done this way because all these files are required to get the latest snapshot of the backup file and they should not be removed from the backup server by the retention area cleanup routine. All other intermediate delta files are stored in the retention area.

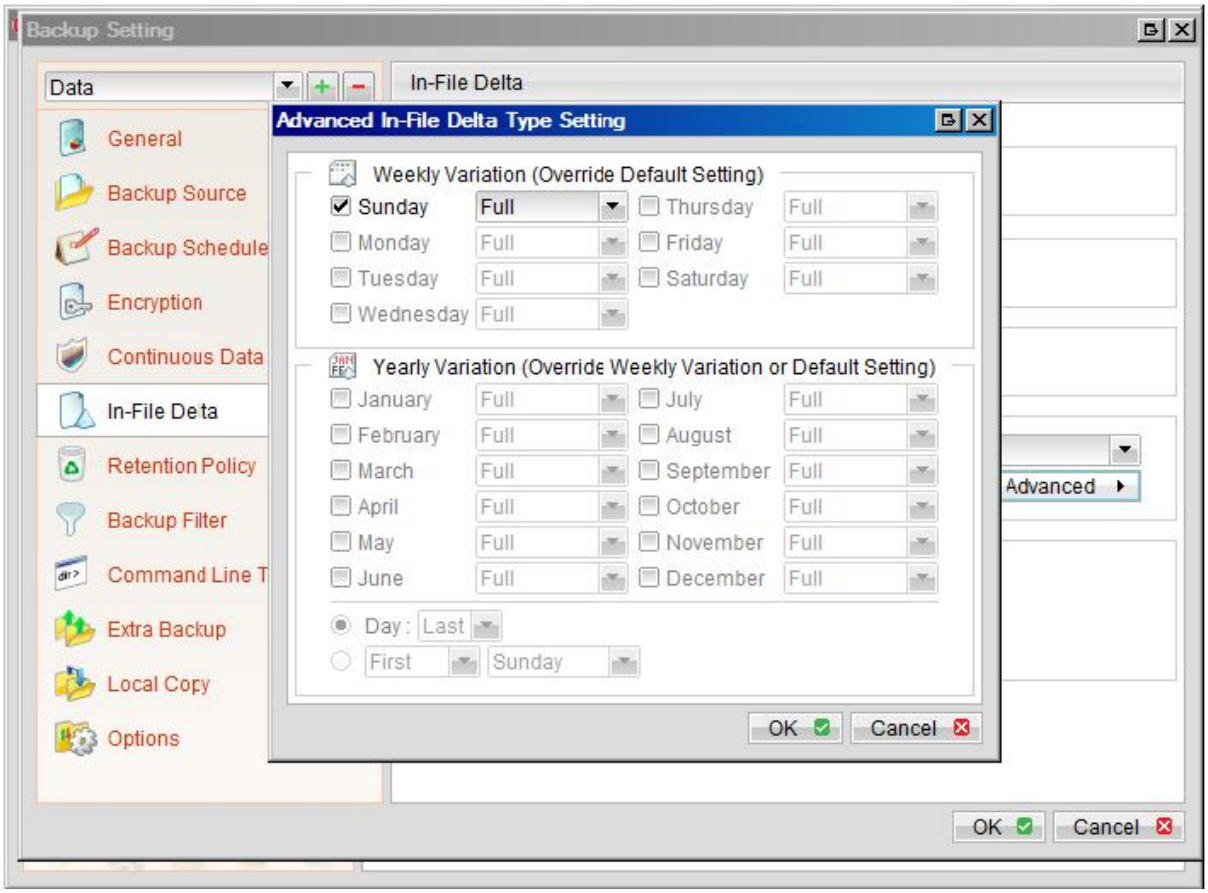
9.1.1.4 Advance In-file Delta Type

[Advanced In-file Delta Type] defines an advance policy, where users can override the default In-file delta setting on specific days in terms of day of a week, or day of a year, for example all Sundays, or the first day of each month.



This is especially useful for users who want to limit their backup on specific day. For example, incremental delta backup on weekdays and differential delta backup on Saturday.

Press the [Advanced] button and the [Advanced In-File Delta Type Setting] dialog will be display.



Menu Items	Description
Weekly Variation (Sunday to Saturday)	Click on the checkbox beside the corresponding day to enable advance In-file delta setting for that day.
Delta type drop down menu (Sunday to Saturday)	Click on the dropdown menu beside the corresponding day to select the delta type for that day.
Yearly Variation (January to December)	Click on the checkbox beside the corresponding day to enable advance In-file delta setting for that day.
Day number (used with yearly variation)	Click on the radio button and dropdown menu to select the day number, of month selected.
Day of week (used with yearly variation)	Click on the radio button and dropdown menus to select the day of week, of the month selected.

9.1.5 Upload full file when

[Upload full file when] defines the rules which Quick Backup will perform a full file backup instead of a delta backup.

Quick Backup will upload a full file when one of the following rules is true:

- When the number of delta files generated (since the last full backup) since the last full file exceeded the [No. of Delta] setting.

- When the delta ratio of the delta file (ratio of delta file size against the full file size) exceeded the [Delta Ratio] setting.

9.1.1.5 No. of Delta

[No. of delta] defines the maximum number of deltas allowed for each full file (within the backup set) before Quick Backup will force a full file upload to the backup server.

For example, if the [No. of delta] is set to 10, and the corresponding file already has 10 deltas saved on the backup server. On the next backup, Quick Backup would upload the full file instead of generating a delta since the [No. of delta] is reached.

This setting is to ensure that there will be a full file backup after a certain number of deltas has been generated (limiting the size of the delta chain).

9.1.2.5 Delta Ratio

[Delta Ratio] defines the maximum 'ratio of change' (delta file size when compare to the last backup) before Quick Backup will force a full file upload to the backup server.

Delta ratio is calculated by dividing the file size of a delta by the file size of the full file (e.g. the percentage of changes detected between the last full backup file and the current file).

For example, if the [Delta Ratio] is set to 50% (default setting), if a file changes by more than 50%, Quick Backup would upload the full file instead of generating a delta since the [Delta Ratio] is reached.

This setting is to ensure that a full file backup is performed for file with significant changes, as it is preferable to upload a full file instead to reduce the time required to restore the file.

10 Backup / Restore Windows System State

This chapter describes in details how to backup and restore Windows System State.

10.1 Supported Versions

The System State backup module is supported for the following Windows platforms:

- Windows XP
- Windows Server 2003 / R2
- Windows Server 2008 / R2
- Windows Small Business Server 2011

10.2 Requirements and Recommendations

For System State backup of **Windows XP or 2003 / R2**, please ensure that the following requirements or recommendations are met:

1. Quick Backup is installed on the computer to be backed up.
2. Sufficient disk spaces are required for the temporary directory (configured in Quick Backup) of the System State backup:
   - Windows XP, 2003 / R2 - usually of size around 2 GB
3. It is recommended that the temporary directory be configured on a local drive.

For System State backup of **Windows 2008 / R2 or SBS 2011**, please ensure that the following requirements or recommendations are met:

4. Quick Backup version 6.3 or above is installed on the computer to be backed up.
5. Sufficient disk spaces are required for the temporary directory (configured in Quick Backup) of the System State backup:
   - Windows 2008 / R2, SBS 2011 - usually of size around 10 GB
6. The following Windows Features are installed on the client computer (under Server Manager):
   - Windows Server Backup Features
     - Windows Server Backup
     - Command-line Tool
   - Windows PowerShell
7. Limitations on the temporary directory (imposed by Microsoft):
   - Temporary directory must be a local or USB drive.
   - Temporary directory can be a non-critical or critical drive.

- Temporary directory can only be set to the root of a drive.
- Shadow Copies storage location of temporary directory must be set to local.

For more details, please refer to Quick Backup Help Centre Article:
http://help.Quick Backup .com/openArticle.aspx?aid=2869

8. It is recommended that the temporary directory be configured on a local drive

10.3 Overview

The following steps take place when a System State backup is performed with Quick Backup:

1. Connection from the backup client to the backup server is established.
2. Download the server file list from the backup server.
3. Commands are issued to create the System State data:
   - Windows XP, 2003 - NTbackup
   - Windows Server 2008, SBS 2011 - Wbadmin
4. System State data is temporarily stored in the temporary directory specified in the backup set.
5. Server and local file lists are compared to determine which file will be uploaded
6. Delta file is generated for modified file (if necessary).
7. Data are encrypted, compressed, and uploaded to the backup server.
8. System State data is removed from the temporary directory specified in the backup set.
9. Backup completed successfully.

10.4 How to backup Windows System State

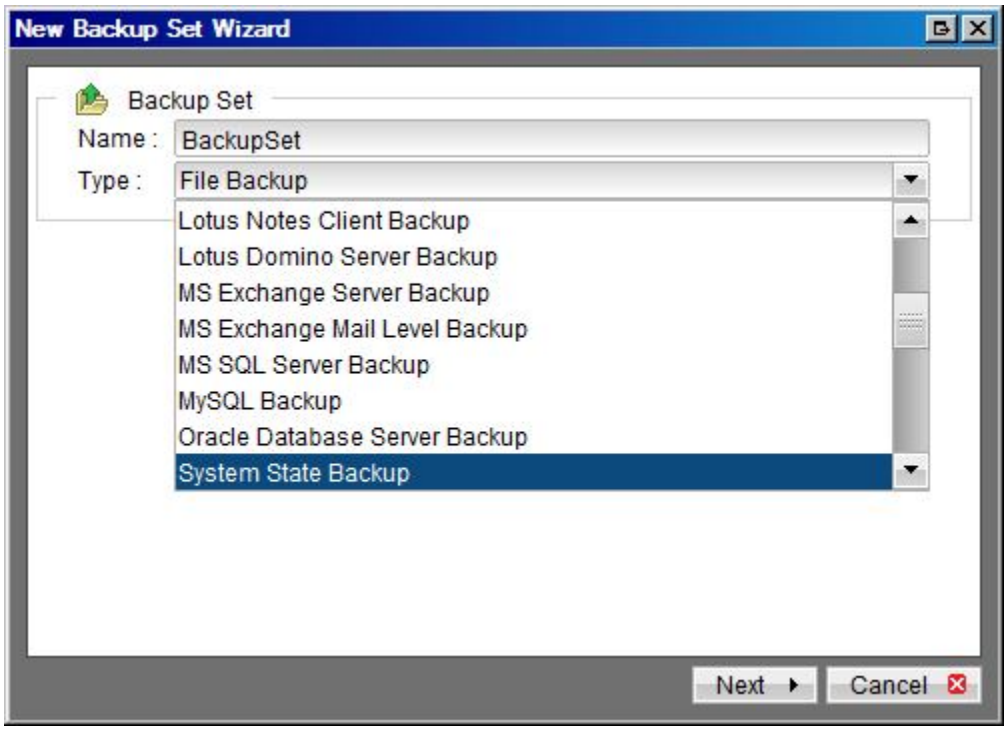
Refer to the follow instructions to backup Windows System State:

10.4.1 For Windows XP, 2003 / R2

1. Login to the backup application's user interface.

2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

3. Create a System State Backup set by selecting [System State Backup] from the backup set type dropdown menu.



4. Select [Next] to proceed.

5. Configure a backup schedule for unattended backups.

6. Select an encryption setting for your backup set.

7. Press the [OK] button to complete the configuration of backup set.

8. Scheduled backup will run automatically if you leave your computer on.

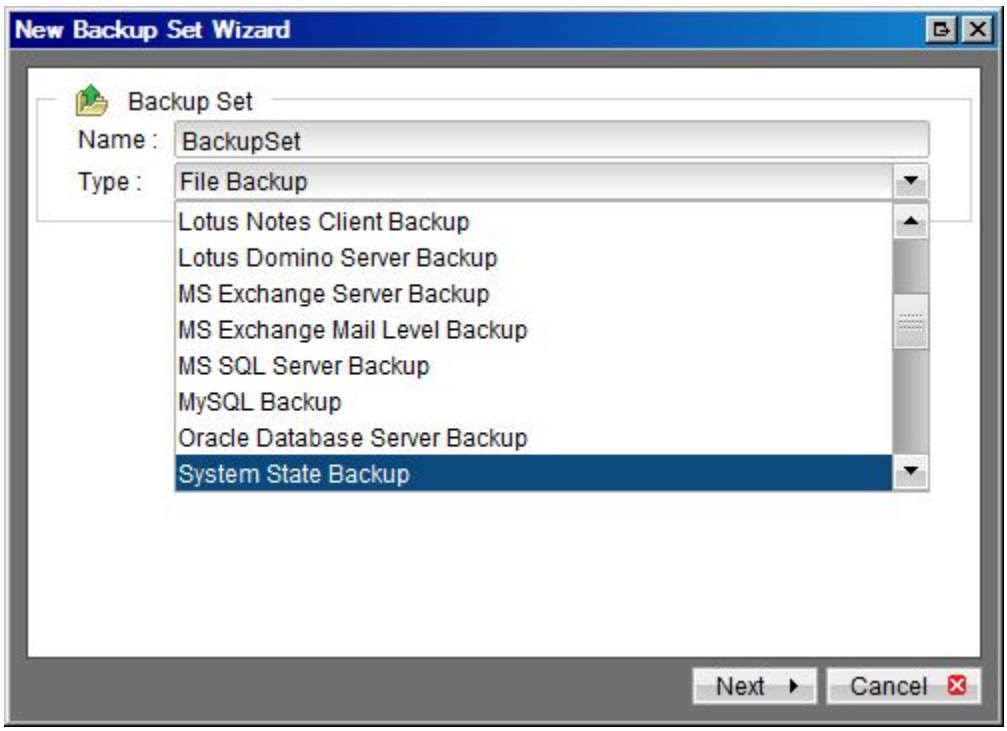
9. To perform a backup immediately, click [Backup] button on the left panel.

10.4.2 For Windows Server 2008 / R2, SBS 2011

1. Login to the backup application's user interface.

2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

3. Create a System State Backup set by selecting [System State Backup] from the backup set type dropdown menu.



4. Select [Next] to proceed.

5. Configure a backup schedule for unattended backups.

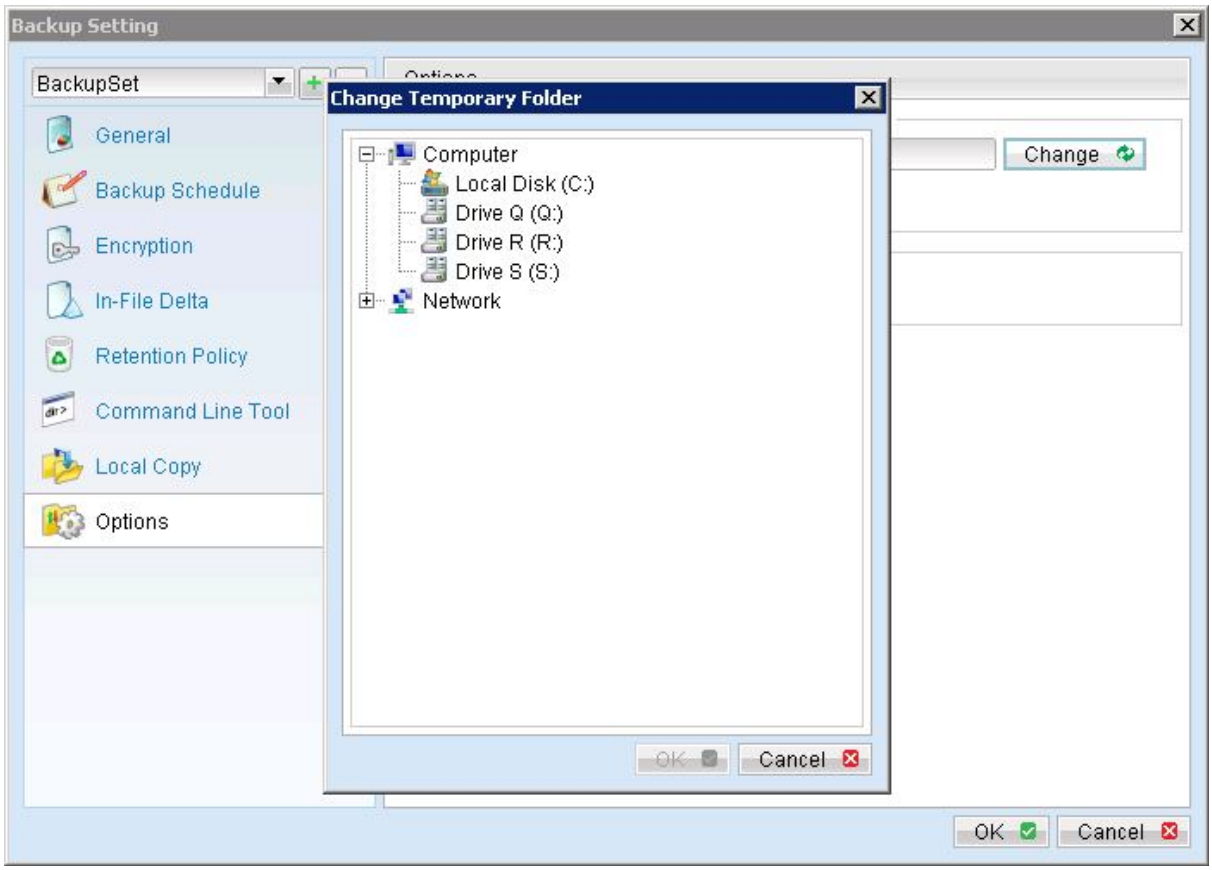
6. Select an encryption setting for your backup set.

7. Press the [OK] button to complete the configuration of backup set.

8. Configure the temporary directory of the System State backup set.

9. On the Quick Backup main menu, press [Backup Setting], then [Options].

10. Click [Change] and select the temporary volume for backup.



11. Scheduled backup will run automatically if you leave your computer on.

12. To perform a backup immediately, click [Backup] button on the left panel.

10.5 How to restore Windows System State

10.5.1 For Windows XP, 2003 / R2

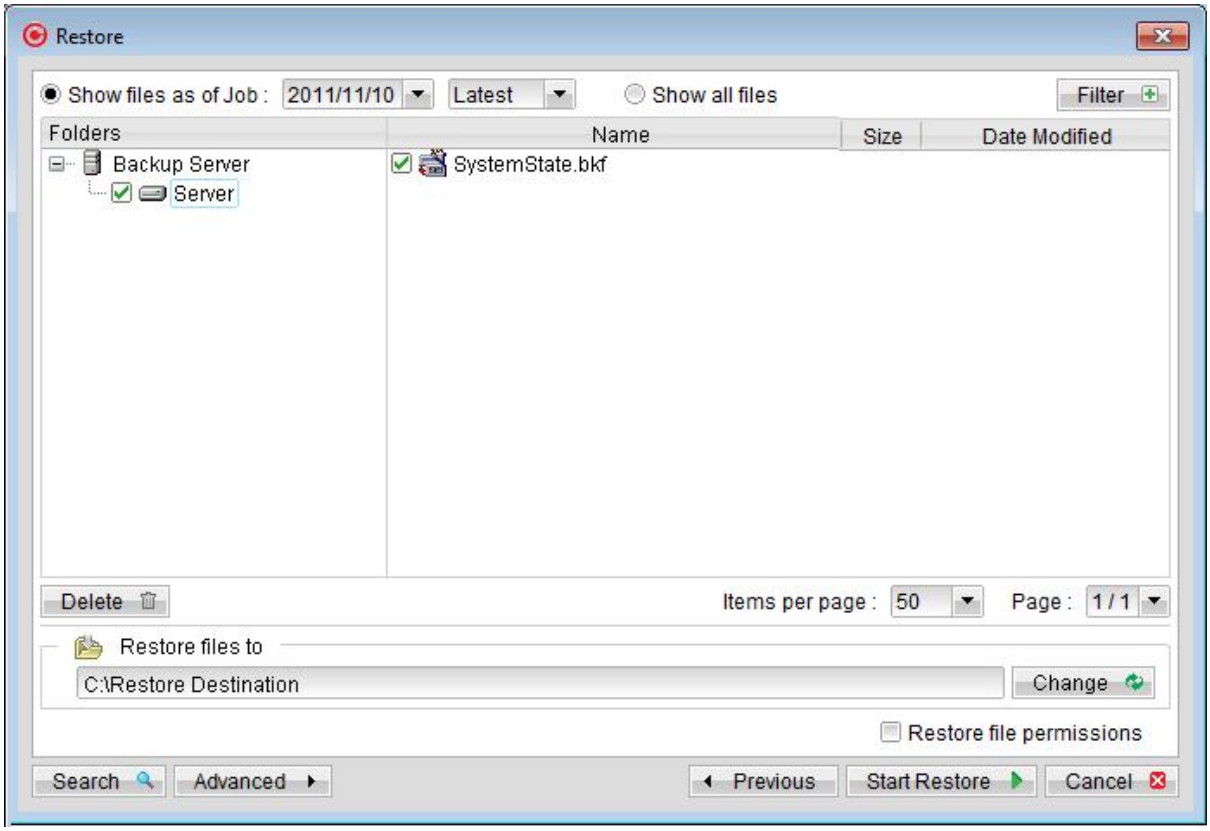
Refer to the follow instructions to restore Windows System State on Windows XP, Server 2003 / R2:

1. Install Quick Backup on the machine to be restored to.

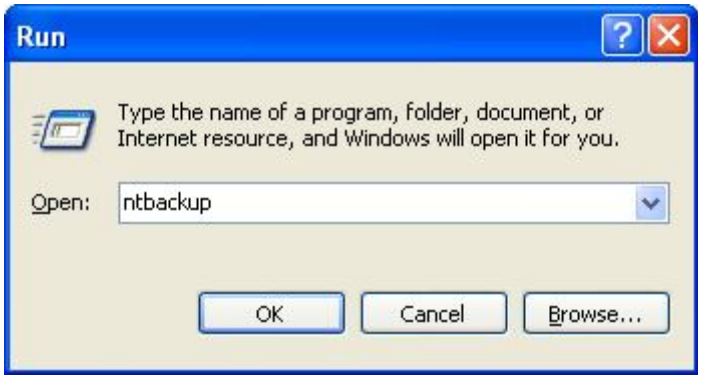
2. Login to the backup application's user interface.

3. Select the [Restore] button and the corresponding backup set.

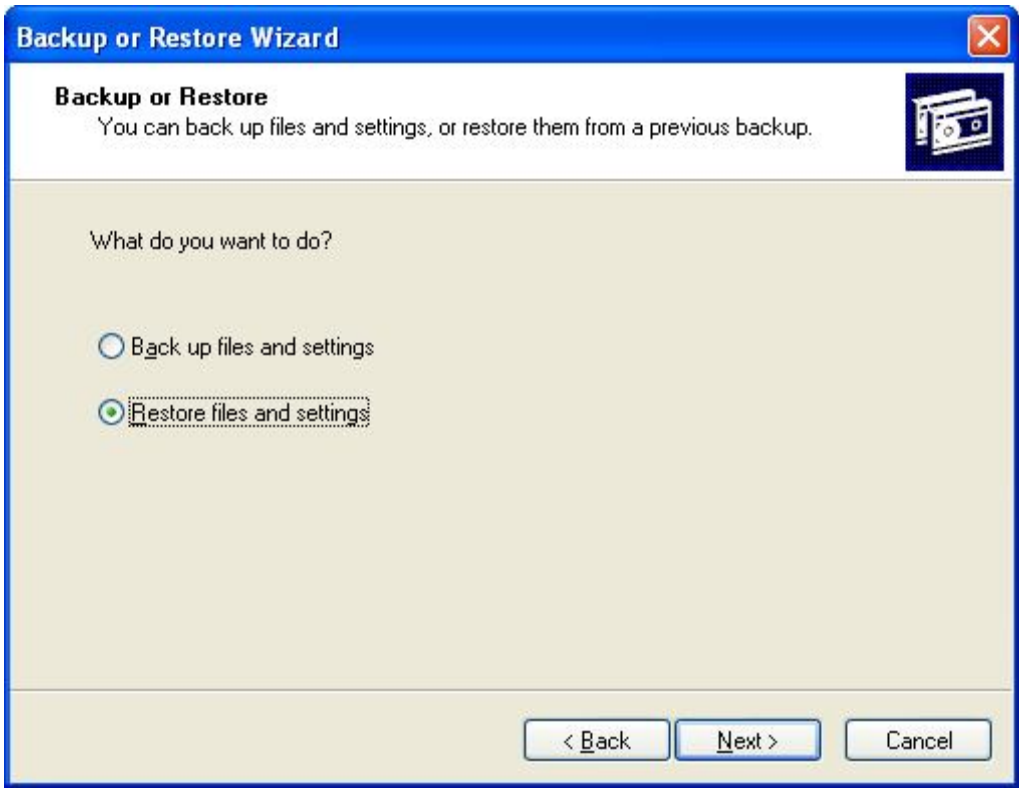
4. Select the System State file (SystemState.bkf) to be restored and its restore destination.



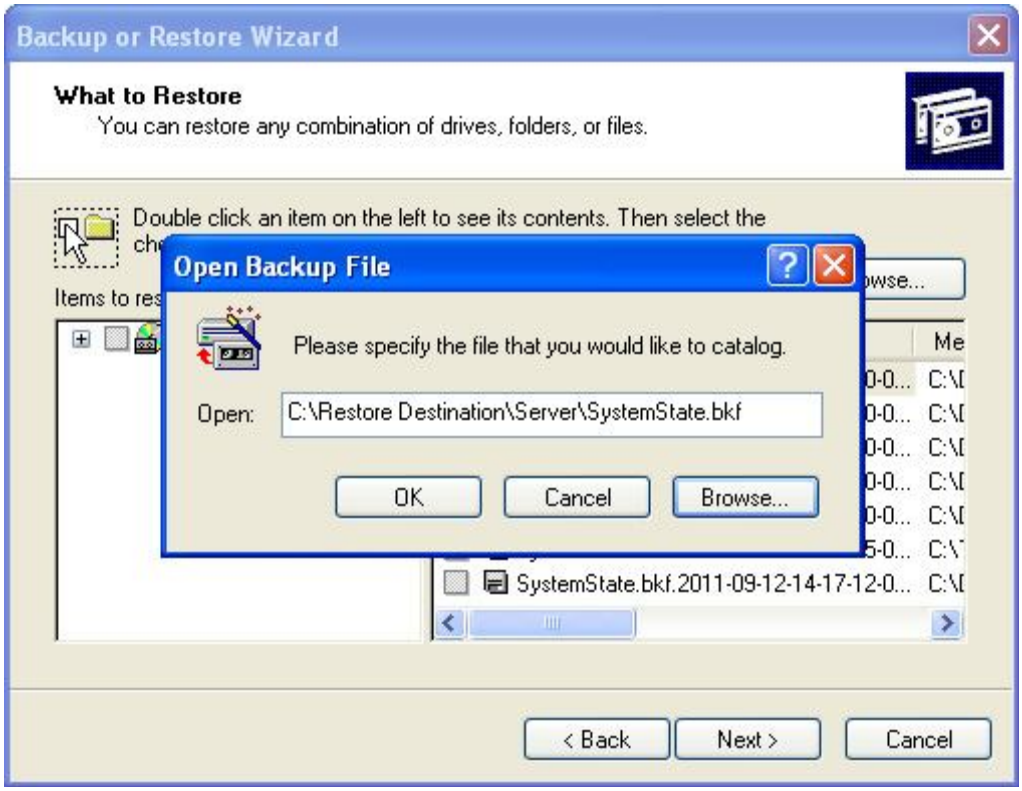
5. Open NTBackup, in the Windows Start menu, click [Run…] and type in ntbackup.



6. Press [Next] and select [Restore files and settings]

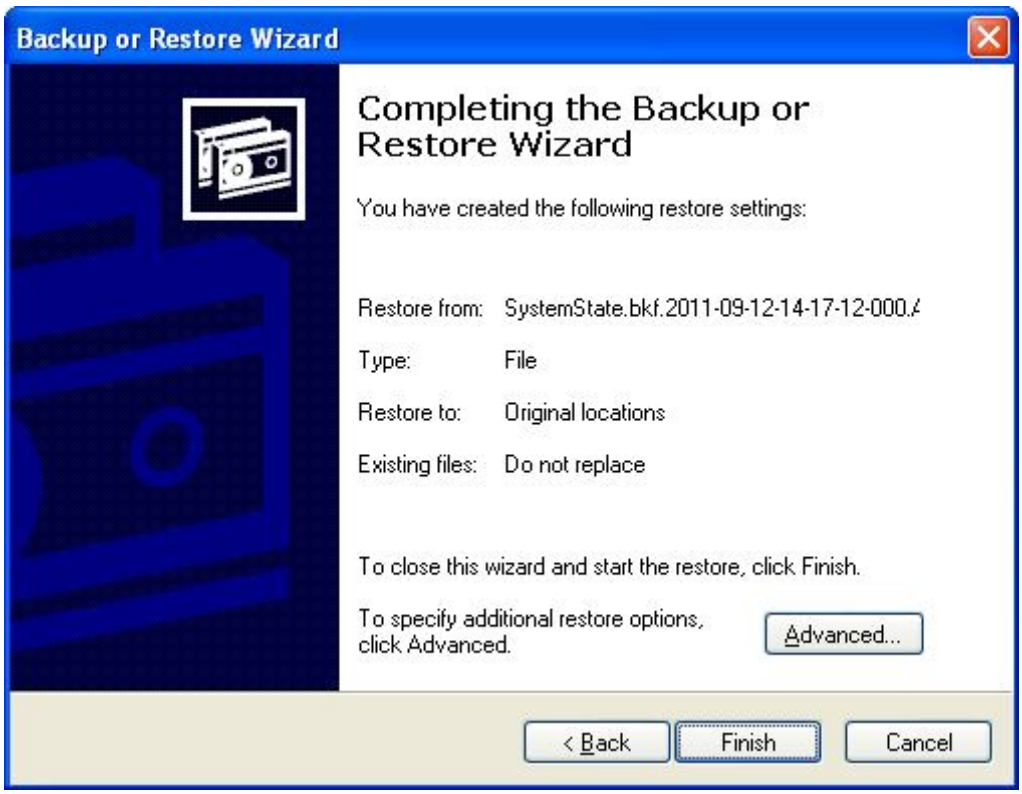

Backup or Restore Wizard
Backup or Restore
You can back up files and settings, or restore them from a previous backup.
What do you want to do?
Back up files and settings
Restore files and settings
< Back
Next >
Cancel

7. Click [Browse], browse to the SystemState.bkf file which you have restored via Quick Backup, then press [OK].



8. Expand and select the corresponding System State file from the left panel, press [Next] afterward.

9. Review the settings, press [Finish] to begin the restore process.


Backup or Restore Wizard
Completing the Backup or Restore Wizard
You have created the following restore settings:
Restore from: SystemState.bkf.2011-09-12-14-17-12-000.
Type: File
Restore to: Original locations
Existing files: Do not replace
To close this wizard and start the restore, click Finish.
To specify additional restore options, click Advanced.
Advanced...
< Back
Finish
Cancel

10. The restore process is now completed.

10.5.2 For Windows 2008 / R2, SBS 2011

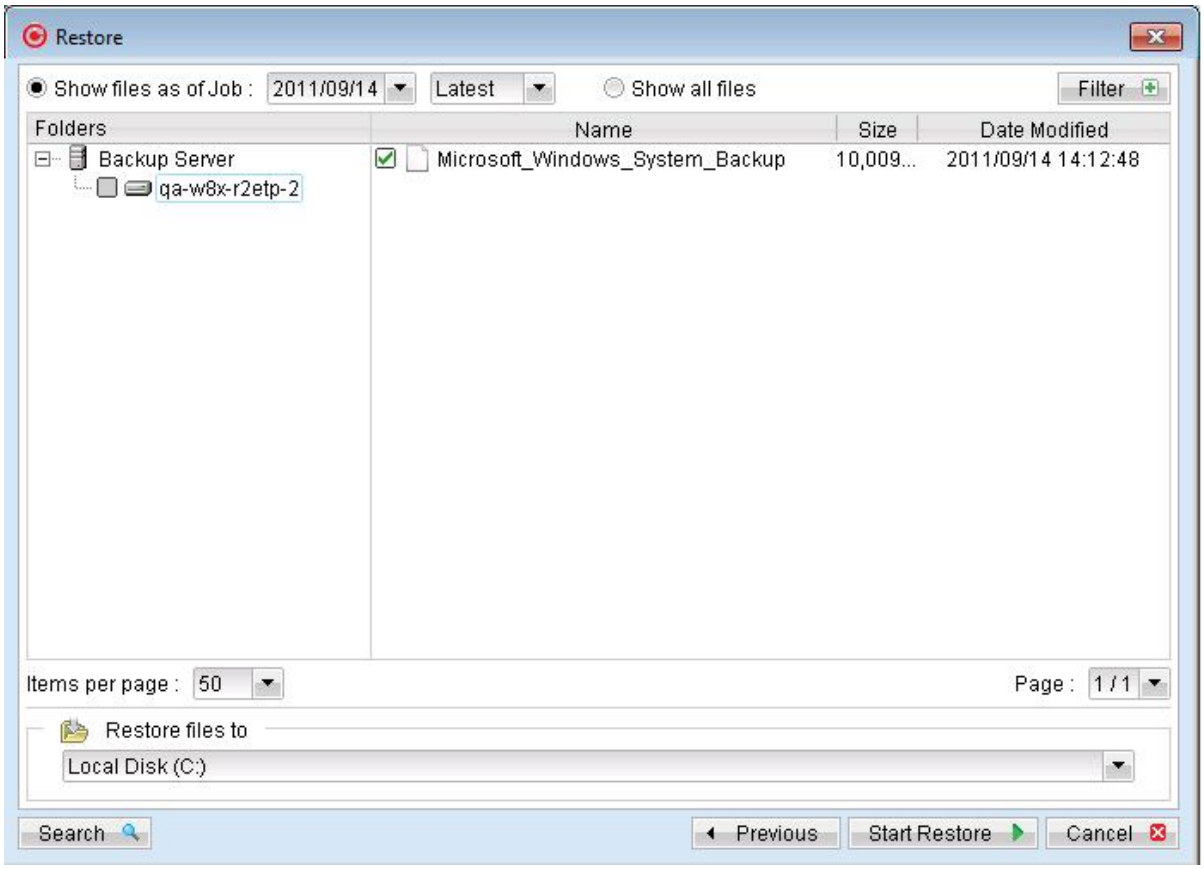
Refer to the follow instructions to restore Windows System State on Windows Server 2008 / R2, SBS 2011:

1. Install Quick Backup on the machine to be restored to.

2. Login to the backup application's user interface.

3. Select the [Restore] button and the corresponding backup set.

4. Select the System State file to be restored and its restore destination.



5. Insert the Windows Setup Disc into the CD / DVD drive

6. Restart the computer. In some case, you need to press the required key to boot up the server from disc; the [Install Windows Wizard] should appear.

7. Specify the language settings, and then click [Next].

8. Click [Repair your computer].

9. Setup will search the hard disk drives for existing Windows installation, then displays the result in [System Recovery Options].

   If you are recovering the operating system onto a new hardware setup, the list will be empty (e.g. there is no existing operating system).

   Click [Next] afterward.

10. On the [System Recovery Options] page, click [Windows Complete PC Restore]. This opens the Windows Complete PC Restore Wizard.

11. Perform one of the following actions:

    - Click [Use the latest available backup (recommended)] and then click [Next].

    - Click [Restore a different backup] and then click [Next].

12. If you choose to restore a different backup, please perform one of the following actions on the [Select the location of the backup] page:

    - Click the computer that contains the backup that you want to use, and then click [Next]. Then, on the [Select the backup to restore] page, click the backup that you want to use, and then click [Next].

    - Click [Advanced] to browse for a backup on the network, and then click [Next].

13. On the [Choose how to restore the backup] page, perform the following optional tasks, and then click [Next]:

    - Select the [Format and repartition disks] check box to delete existing partitions and reformat the destination disks to be the same as the backup.

      This enables the [Exclude disks] button. Click this button and then select the check boxes associated with any disks that you want to exclude from being formatted and partitioned. The disk that contains the backup that you are using is automatically excluded.

      Note:
      Unless a disk is excluded, data on it can be lost – regardless of whether it was part of the backup or whether it has volumes that are being restored.

      In [Exclude disks], if you do not see all the disks that are attached to the computer, you might need to install the associated drivers for the storage device.

    - Select the [Only restore system disk] check box to perform an operating system-only recovery.

    - Click [Install drivers] to install drivers for the hardware that you are recovering to.

- Click [Advanced] to specify whether the computer is restarted and the disks are checked for errors immediately after the recovery.

14. Confirm the details for the restoration, and then click [Finish].

10.5.3 For Windows 2008 / R2 Domain Controller

Refer to the follow instructions to restore Windows System State on Windows Server 2008 / R2 Domain Controller:

Important:
Authoritative restore of Windows 2008 Domain Controller is required only if you need to restore deleted Active Directories objects.

Please follow the instructions below to restore a system state backup to a Windows 2008 Domain Controller:

1. Reboot the Windows Server 2008 / R2 Domain Controller in Directory Service Repair Mode (DSRM):

    - Add the safeboot option to the default boot loader. In command prompt, type in the following command:

```
>bcdedit /set safeboot disrepair
```

    - Reboot the computer.

2. Perform the restore on the Domain Controller:

    - Open command prompt and type the following:

```
>wbadmin get versions
```

    This will list all the known backups available.

    - Type the following command to perform an authoritative restore:

```
>wbadmin start systemstaterecovery –version:<backup_version> -authsysvol
```

    For non-authoritative restore, please type the following command:

```
>wbadmin start systemstaterecovery –version:<backup_version> -authsysvol
```

<backup version> is the identifier of one of the backup snapshots listed in the previous step.

3. Reboot the Windows Server 2008 / R2 Domain Controller in Normal Mode:

   - Remove the safeboot option to the default boot loader. In command prompt, type in the following command:

```
>Bcdedit /deletevalue safeboot
```

   - Reboot the computer.

4. The restore process is now completed.

11 Backup / Restore System with Microsoft Windows System Backup

This chapter describes in details how to use Quick Backup to backup your Microsoft Windows System and how you can restore them from backup files. This feature only works on Microsoft Windows Vista Business / Enterprise / Ultimate Edition, Windows 7 and Windows Server 2008.

11.1 Requirements

To backup / restore Microsoft Windows Systems Backup, please make sure that the following requirements are met:

1. The computer is using one of the following operating systems:

   - Windows Vista Business / Enterprise / Ultimate Edition
   - Windows 7 Business / Enterprise / Ultimate Edition
   - Windows Server 2008

2. Quick Backup must be installed on the computer to be backed up.

3. You must install the Windows Server Backup, Command-line Tools, and Windows PowerShell Items that are available in the [Add Feature Wizard] in [Server Manager]. This installs the following tools:

   - Windows Server Backup Microsoft Management Console (MMC) snap-in.
   - Wbadmin command-line tool.
   - Windows Server Backup cmdlets (Windows PowerShell Commands)

4. System images generated by Windows Server Backup will be backed up to a temporary directory before they are sent to Quick Backup Server. Please make sure you have sufficient space on your computer to store these data when you run the backup job.

11.2 Overview

Quick Backup will backup your system by taking the following steps:

1. Before running any backup activities, Quick Backup will run all Pre-Commands of the backup set.
2. Quick Backup will issue a system backup command to backup the volume(s) selected in backup source to a set of files and save it in the [Windows Image Backup] directory under the temporary directory specified in the backup set settings.
3. After all files have been spooled to the [WindowsImageBackup] directories, Quick Backup will run all Post-Commands of the backup set.
4. Upload all files copied to the temporary directory to Quick Backup Server.

For windows, there are 3 major partition types:

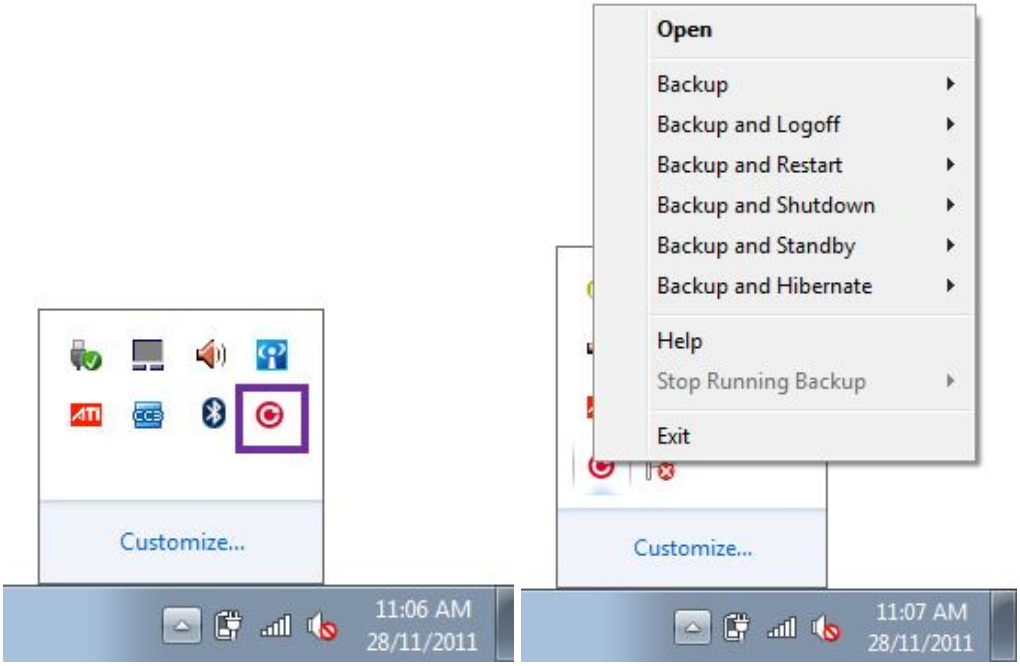
1. System Partition – a disk partition that contains the boot loader, i.e. NTLDR in WinXp and earlier or bootmgr for Windows Vista/2008/7.
2. Boot Partition – a disk partition that contains the Windows operating system files and its support files.
3. System Reserved Partition – a disk partition introduced in Windows 7 and 2008 R2. It contains the Windows Recovery Environment, boot loader and BitLocker related files. This partition is created when the OS is installed on hard disk with single partition scheme or unallocated space on the hard drive.

11.3 How to backup system with Microsoft Windows System Backup

Please follow the instructions below to backup your Microsoft Windows Server 2008 or Windows Vista Business/Enterprise/Ultimate Edition using Quick Backup.

1. Open Quick Backup.

   Right click Quick Backup icon available in the system tray and choose [Open].

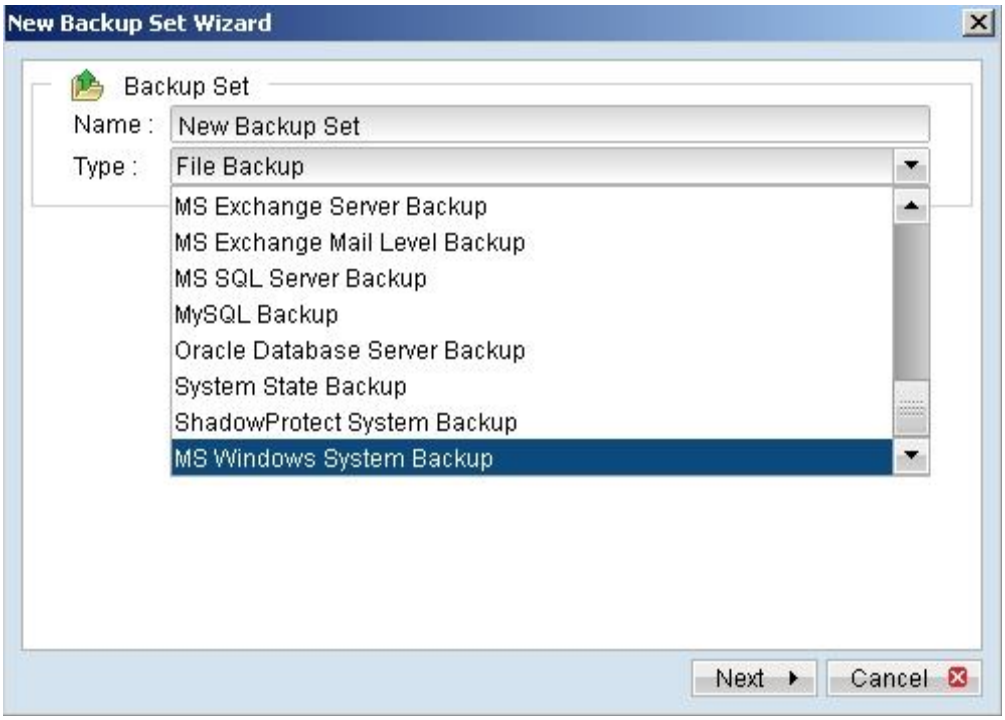


2. Create a backup set.

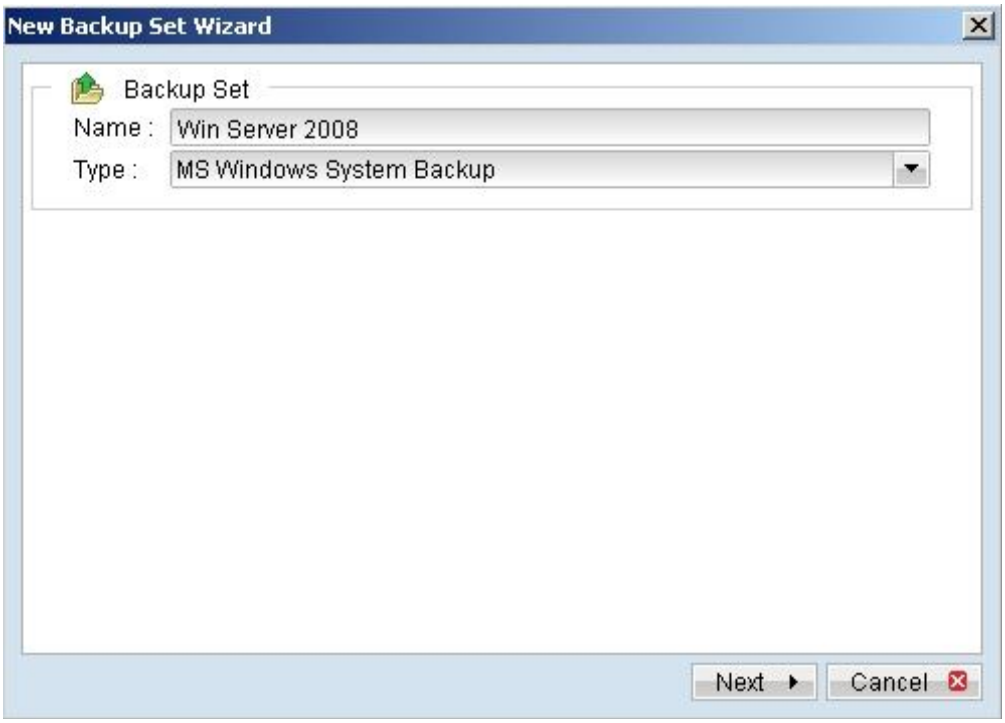
   i. To start setting up backup sets, click the button to open the [Backup Setting] dialog.

   ii. On the left panel, press the button to create a new backup set.

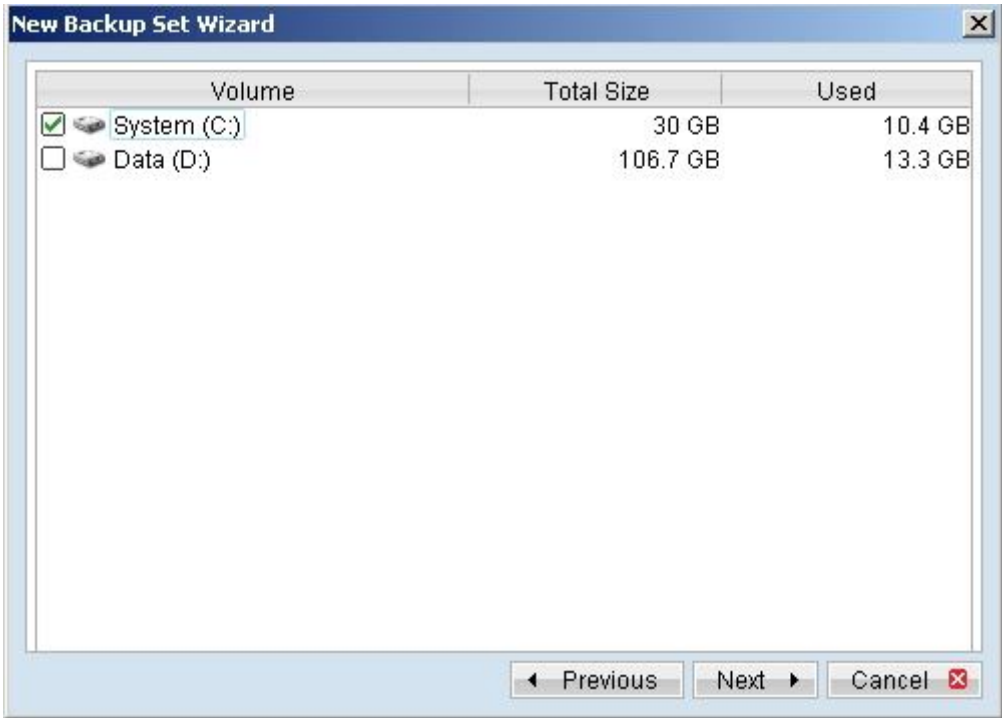
iii. On the dialog, choose [MS Windows System Backup] as the [Type].



iv. Enter a name for your backup set.

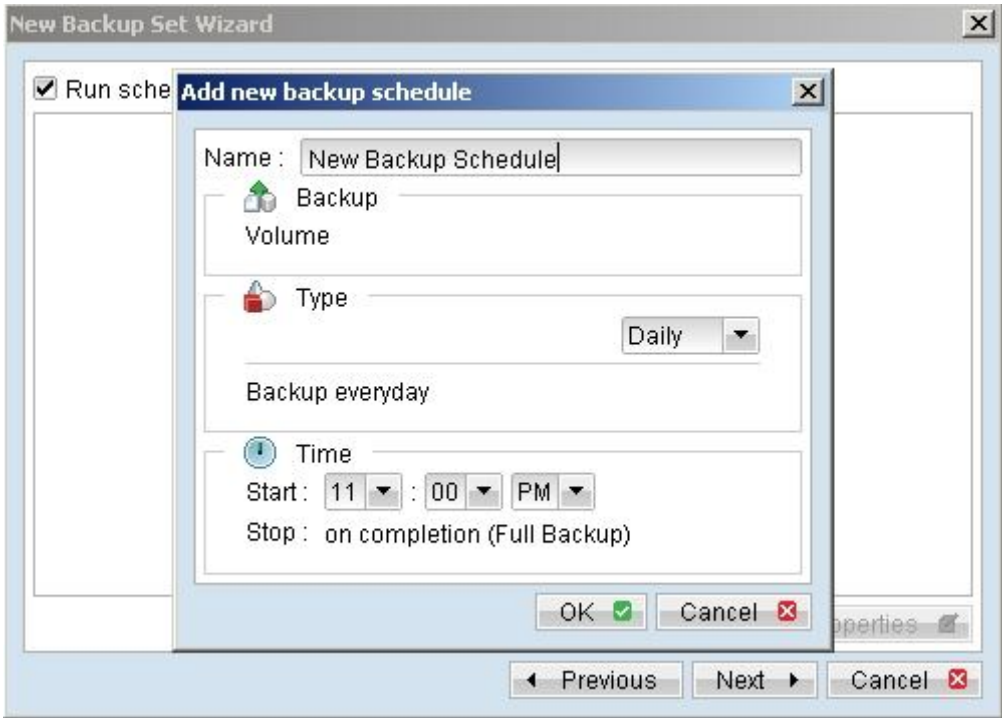


v. Select the volume(s) you want to backup.

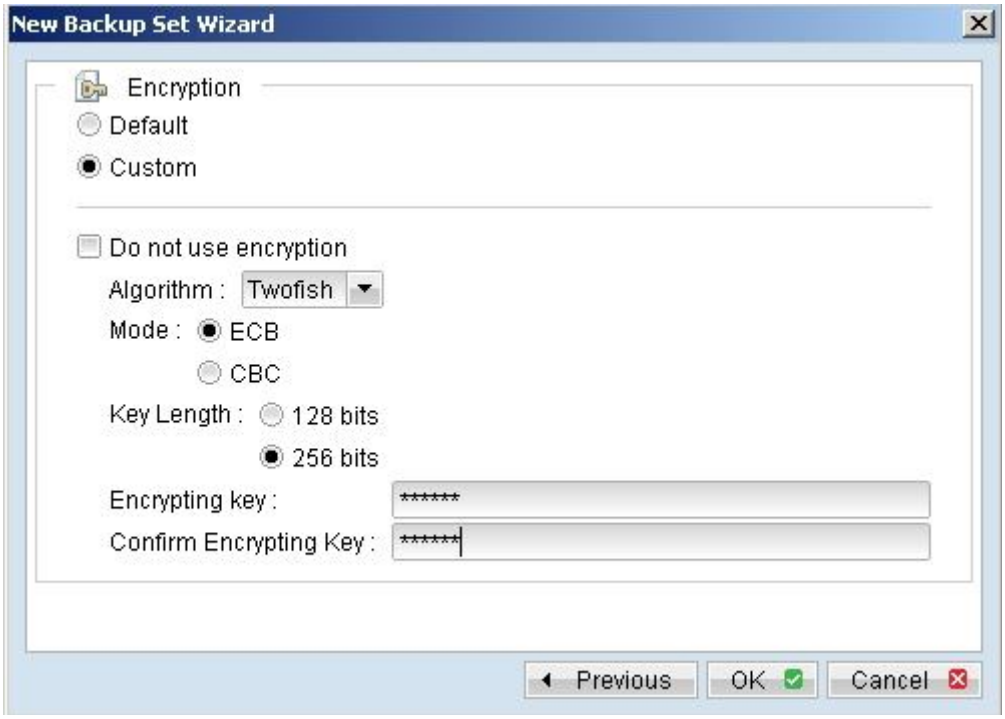


To perform a Complete Windows System Backup, it is highly recommended to enable the [Include all critical volumes] option. By the use of this option, it will select all partitions that are required for system recovery, this includes the system partition, boot partition, system reserved partition and other partitions that contain critical system data. This can avoid any essential volume missing from the Windows System Backup.

vi. Set the backup schedule.



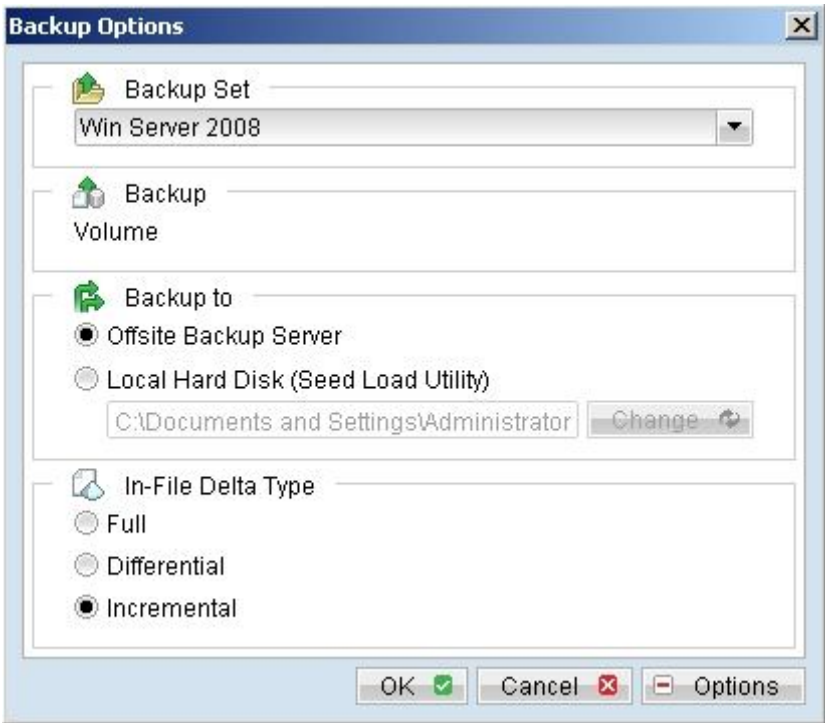
vii. Set the encryption algorithm, encryption mode and encrypting key for this backup set.



3. Run Backup

i. Press the [Backup] button on the main page of Quick Backup dialog.

ii. Select the backup set you want to run and select [Offsite Backup Server] to start backing up your files to Quick Backup Server. IF applicable, you can change the In-File Delta Type also.



iii. Click [OK] to start backing up your files to Quick Backup Server.

11.4 How to restore system with Microsoft Windows System Backup

Please follow the instructions below to restore your Microsoft Windows System from Quick Backup Server.

Recover Volumes with Recovery Wizard

1. Download the backup file (Microsoft_Windows_System_Backup) from Quick Backup Server.

2. From the [Start] menu, click [Administrative Tools], and then click [Windows Server Backup].

3. In the [Actions] panel of the snap-in default page, under [Windows Server Backup], click [Recover.] This opens the Recovery Wizard.

4. On the Getting started] page, specify whether you will recover volumes from backups stored on this computer or another computer, and then click [Next].

5. If you are recovering volumes from backups stored on another computer, please do the following, and then click [Next]:

   i. On the [Specify location type] page, specify the location that you want to restore from a local drive.

   ii. On the [Select backup location] page, select the location of the backup from the drop-down list.

6. Click [Next] to continue.

7. For recovery either from the local computer or another computer, on the [Select backup date] page, select the date from the calendar and the time from the drop-down list of backup you want to restore from.

8. On the [Select recovery type] page, click [Volumes], and then click [Next].

9. On the [Select volumes] page, select the check boxes associated with the volumes in the [Source Volume] column that you want to recover. Then, from the associated drop-down list in the [Destination Volume] column, select the location that you want to recover the volume to and click [Next].

   Note: You will receive a message that any data on the destination volume will be lost when you perform the recovery. Make sure that the destination volume is empty or does not contain information that you will need later.

10. On the [Confirmation] page, review the details, and then click [Recover] to restore the specified volumes.

11. On the [Recovery progress] page, you can view the status of the recovery operation and whether or not it was successfully completed.

    Note: To recover volumes from a backup using Windows SERVER Backup, you must be a member of the Backup Operators or Administrators group, or you must

have been delegated the appropriate authority. As a security best practice, you should consider to use [Run as] command to perform this procedure.

Recover Operating System/Full Server with Install Windows Wizard

1. Insert the Windows Setup disc into the CD or DVD drive and turn on the computer. If needed, press the required key to boot from the disc. The [Install Windows] Wizard should appear.

2. Specify language settings, and then click [Next].

3. Click [Repair your computer].

4. The Setup Wizard will search the hard disk(s) for any existing Windows installation and then display the result. If you are recovering the operating system onto separate hardware, the list should be empty (there should be no operating system on the computer) and then click [Next].

5. On the [System Recovery Options] page, click [Windows Complete PC Restore]. This opens the Windows Complete PC Restore Wizard.

6. Perform one of the following actions:

    - Click [Use the latest available backup (recommended)] and then click [Next].
    - Click [Restore a different backup] and then click [Next].

7. If you choose to restore a different backup, please perform one of the following actions on the [Select the location of the backup] page:

    - Click the computer that contains the backup that you want to use, and then click [Next]. Then, on the [Select the backup to restore] page, click the backup that you want to use and then click [Next].
    - Click [Advanced] to browse for a backup on the network, and then click [Next].

8. On the [Choose how to restore the backup] page, do the following optional tasks, and then click [Next]:

    - Select the [Format and repartition disks] check box to delete existing partitions and reformat the destination disks to be the same as the backup. This enables the [exclude disks] button. Click this button and then select the check boxes associated with any disks that you want to exclude from being formatted and partitioned. The disk that contains the backup that you are using is automatically excluded.
    - Select the [Only restore system disks] check box to perform an operating system – only restore.
    - Click [Install drivers] to install device drivers for the hardware that you are recovering to.
    - Click [Advanced] to specify whether the computer is restarted and the disks are checked for errors immediately after the recovery.

9. Confirm the details for the restoration, and then click [Finish] to complete the process.

Recover Volumes with the sub command

You can recover volumes with the following sub command:

Wbadmin start recovery –version: <VersionIdentifiers>
-itemtype:Volume –items:<VolumesToRecover>
-backupTarget: <VolumeHosting Backup>
-recoveryTarget:<TargetVolumeForRecovery>

Parameter	Descriptions
VersionIdentifiers	**Specifies the version identifier of the backup to recover in MM/DD/YYYY-HH:MM format. If you do not know the version identifier, type [wbadmin get versions]**
VolumesToRecover	**Specifies a comma-delimited list of volumes.**
VolumesHostingBackup	**Specifies the storage location that contains the backup that you want to recover**
TargetVolumeForRecovery	**Specify the volume drive letter of the alternate volume to restore to.**

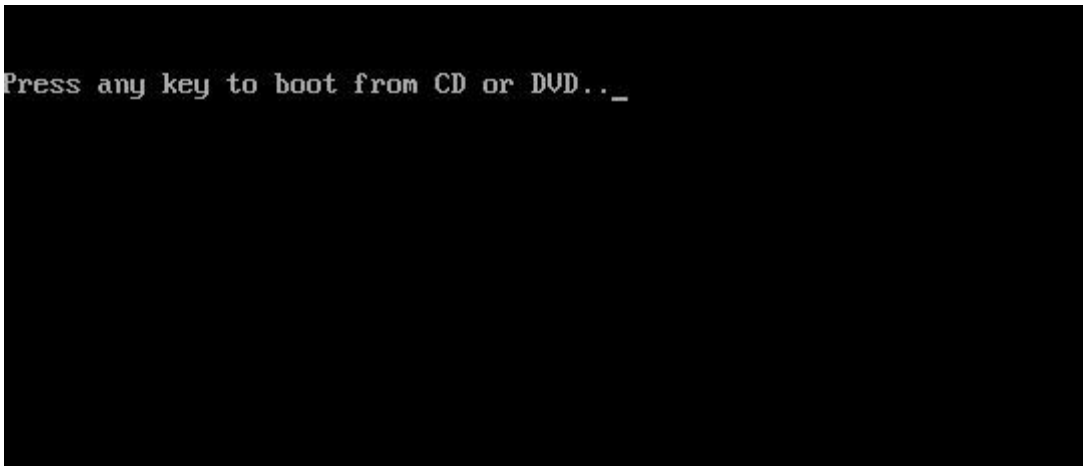
For example,

Wbadmin start recovery –VersionIdentifiers:03/31/2009-09:00
–itemType:Volume –items:D: -backupTarget:E: -recoveryTarget:F:

11.5 How to perform Complete PC Restore

Please do the followings to perform complete PC Restore within the Windows Recovery Environment (Windows Vista / 7 only):

1. Insert Windows DVD into the DVD drive and turn on the computer. You will see that a bootable DVD is inserted.



2. Press any key to boot the computer from the Windows DVD. You should now see a black screen with a white status bar at the bottom stating [Windows is loading files…]. After a while, the status bar will turn completely white and you will see a screen stating that Windows is loading.

Note: It is possible that the DVD came with your computer does not allow you to boot off from it. If this is the case, then your computer manufacture most likely installed the Windows Recovery Environment directly to a small partition on your hard drive. To access this partition, you would slowly tap the [F8] key on your keyboard after the BIOS information clears from your screen until you see the Windows startup menu. From this menu use your arrow keys to select the option for the Windows Recovery Environment and press the enter key on your keyboard.

3. Configure the [Language to install], [Time and currency format], and [Keyboard or input method] options. Then, press the [Next] button.

Install Windows
Windows Vista
Language to install: English
Time and currency format: English (United States)
Keyboard or input method: US
Enter your language and other preferences and click "Next" to continue.
Copyright © 2006 Microsoft Corporation. All rights reserved.
Next

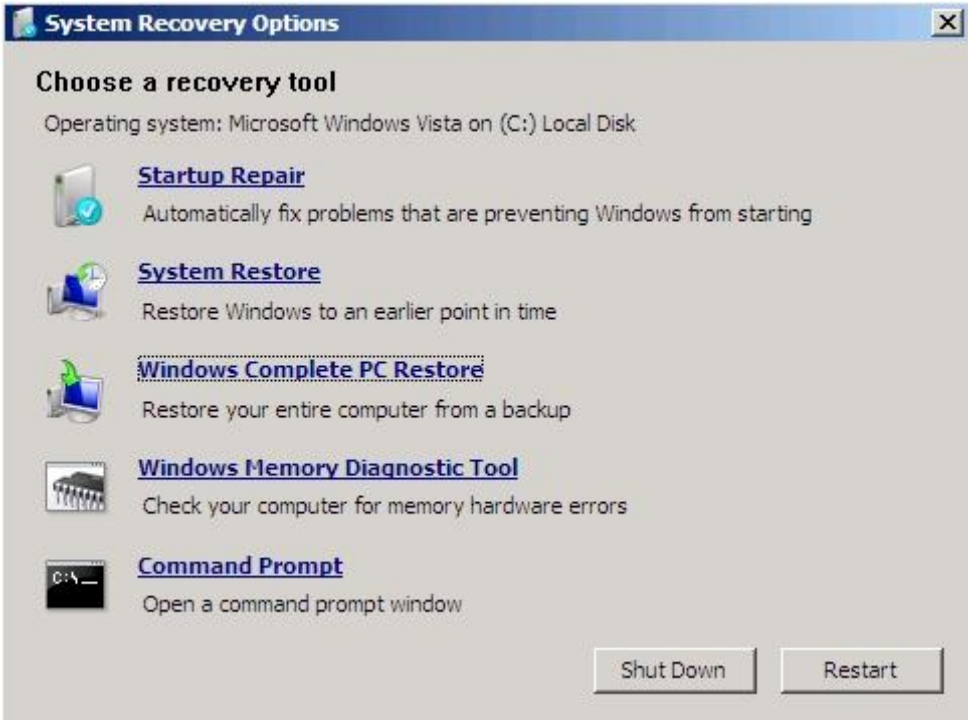
4. Click [Repair your computer].

5. The [System Recovery Options] dialog box will be shown. Select the windows installation you would like to repair.

System Recovery Options
Select an operating system to repair and click Next. Only Windows Vista operating systems are listed and can be repaired.
Operating System
Partition Size
Location
Microsoft Windows Vista
51197 MB
(C:) Local Disk
If you do not see your operating system listed, click Load Drivers to load drivers for your hard disks.
Load Drivers
Next >

Note: If there are drivers you need to load in order for Windows to access any of your drives or other components, then you should click on the [Load Drivers] button to load them. When ready, press the [Next] button to continue. If the repair process does not detect any problems starting Windows, it will display a list of available recovery tools. If it does detect a problem it will attempt to perform a Startup Repair to automatically fix these problems. Click on the [Cancel] button and select the [View advanced options for system recovery and support] option to see the list of recovery tools.

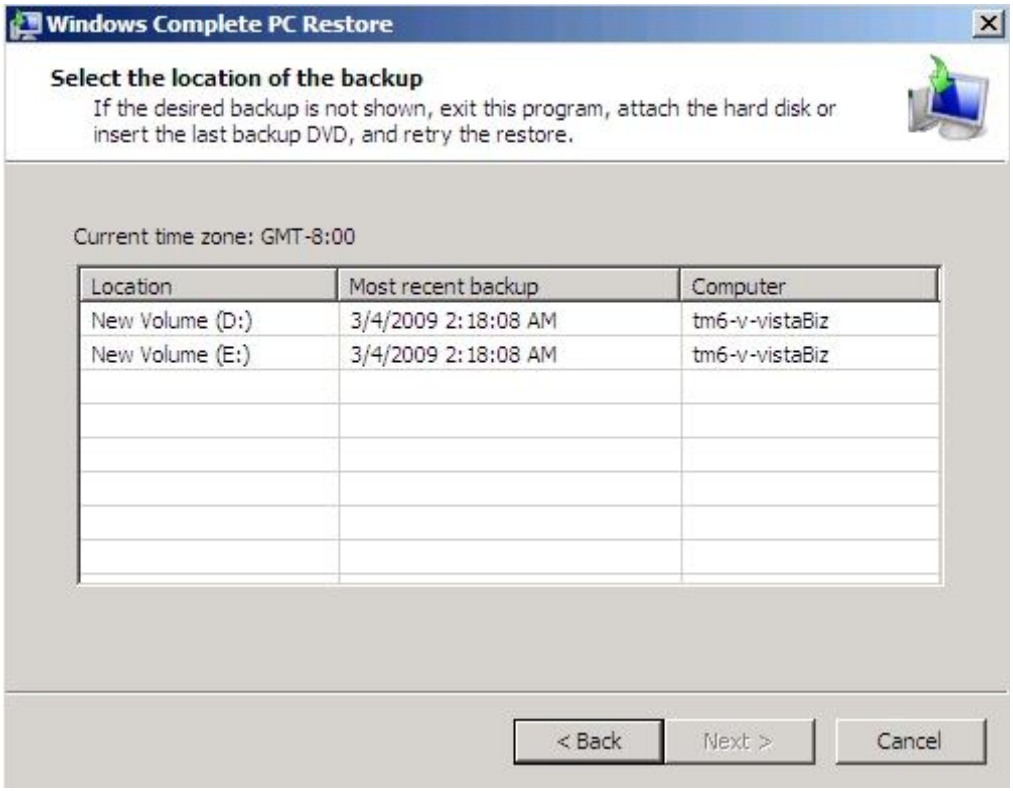
6. Click on the [Windows Complete PC Restore] option.


System Recovery Options
Choose a recovery tool
Operating system: Microsoft Windows Vista on (C:) Local Disk
Startup Repair
Automatically fix problems that are preventing Windows from starting
System Restore
Restore Windows to an earlier point in time
Windows Complete PC Restore
Restore your entire computer from a backup
Windows Memory Diagnostic Tool
Check your computer for memory hardware errors
Command Prompt
Open a command prompt window
Shut Down
Restart

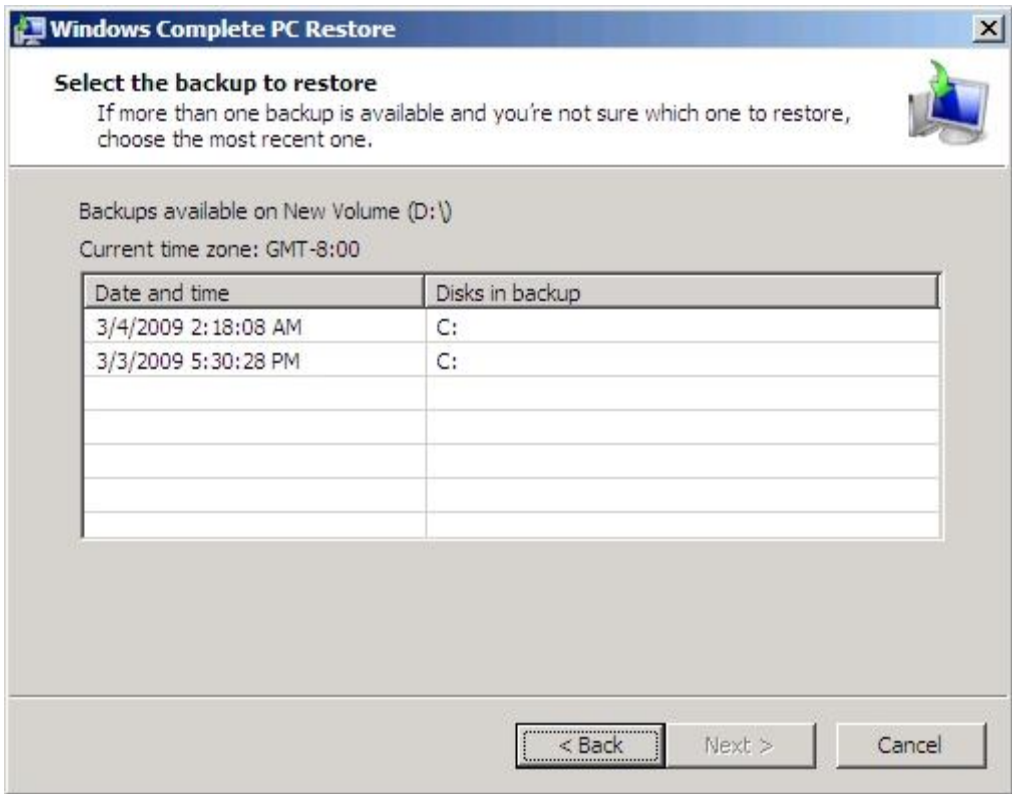
7. Complete PC Restore will search your hard drives and DVD media for any saved backup image. If none are found, a message will appear stating that no backups could be found. On the other hand, if a backup was found in one of your drives or the inserted media, you will see a screen with the latest backup selected.

Windows Complete PC Restore
Restore your entire computer from a backup
All programs and files on your computer will be erased and then the files and the programs will be restored from the backup.
Restore the following backup (recommended)
Location:
New Volume (D:)
Date and time:
3/4/2009 2:18:08 AM (GMT-8:00)
Computer:
tm6-v-vistaBiz
Restore a different backup
< Back
Next >
Cancel

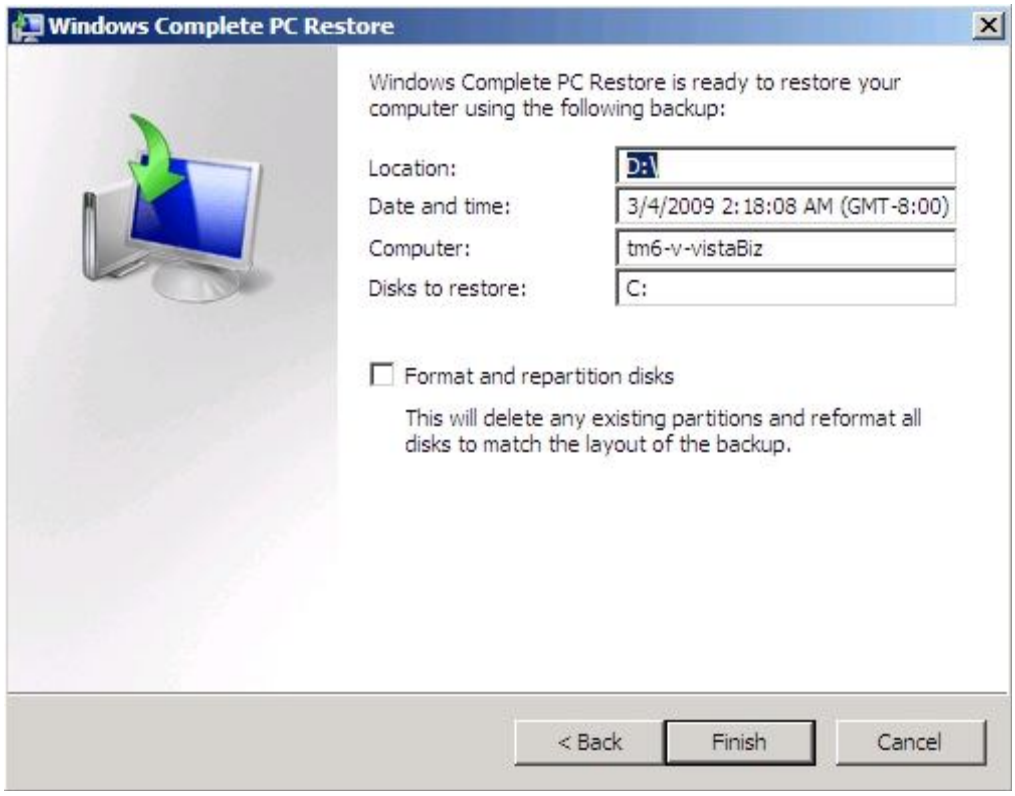
8. If the selected backup is the one you wish to restore, press the [Next] button to continue. If there is a different backup that you would like to use, select the [Restore a different backup] option and press the [Next] button. This will bring up a screen displaying the list of backups you have created in the past.


Windows Complete PC Restore
Select the location of the backup
If the desired backup is not shown, exit this program, attach the hard disk or insert the last backup DVD, and retry the restore.
Current time zone: GMT-8:00
Location
Most recent backup
Computer
New Volume (D:)
3/4/2009 2:18:08 AM
tm6-v-vistaBiz
New Volume (E:)
3/4/2009 2:18:08 AM
tm6-v-vistaBiz
< Back
Next >
Cancel

9. Select the backup that you would like to restore. Then click on the [Next] button. Complete PC Restore will now examine your selected backup and see if there is more than one time you backed your computer to this location. If you have backed up multiple times, it will display an entry for each of them.


Windows Complete PC Restore
Select the backup to restore
If more than one backup is available and you're not sure which one to restore, choose the most recent one.
Backups available on New Volume (D:\)
Current time zone: GMT-8:00
Date and time
Disks in backup
3/4/2009 2:18:08 AM
C:
3/3/2009 5:30:28 PM
C:
< Back
Next >
Cancel

10. During the restoration process, it is recommended to select the most recent snapshot and then press the [Next] button to move on to the next screen.



Note: if you select the [Format and repartition disks] options, Complete PC Restore will repartition and format the hard drive you are restoring to exactly as it was when you made the backup. If you do not choose this method, it will just erase the hard disk and restore the data to it. If you are using the same hard drive that you originally used to backup your computer then you may want to select the option to format and repartition disks. On the other hand, if this is a new hard drive that you have partitioned in a different manner, you should not select this option in order to keep your current disk configuration. It is important to note that if you select either option from the menu, all the data on the disk you are restoring to will be erased. When you are ready to continue, you should click the [Finish] button.

11. A new window is opened stating that all your data will be erased. If you want to continue with the restore, you need to check the checkbox named [I confirm that I want to erase all existing data and restore the backup]. After that, press the [OK] button to continue. Complete PC Restore will now restore the backup on your computer.

Windows Complete PC Restore
Windows is restoring your backup to 3/4/2009 2:18:08 AM (GMT-8:00). This will take several minutes.
Preparing to restore your disks...
Stop restore

12. When the restore is completed, you will see a message stating that it is complete and it will reboot your computer after a certain amount of time. After rebooting your computer, you are able to use the data and configuration restored from the selected backup.

13. The restoration process is now completed successfully.

12 Backup / Restore Windows System with ShadowProtect

This chapter describes in details how to use Quick Backup to backup your Microsoft Windows System by the use of ShadowProtect and how you can restore them from the backup files. Please refer to the website of Storagecraft for the list of operating system supported by ShadowProtect.

12.1 Requirements

Before using ShadowProtect to backup your system, please make sure that the following requirements are met:

1. Quick Backup must be installed on the computer with ShadowProtect installed.
2. System images generated by ShadowProtect will be backed up to a temporary directory before they are sent to Quick Backup Server. Please make sure that you have sufficient space on your computer to store these data when you run the backup job.

12.2 Overview

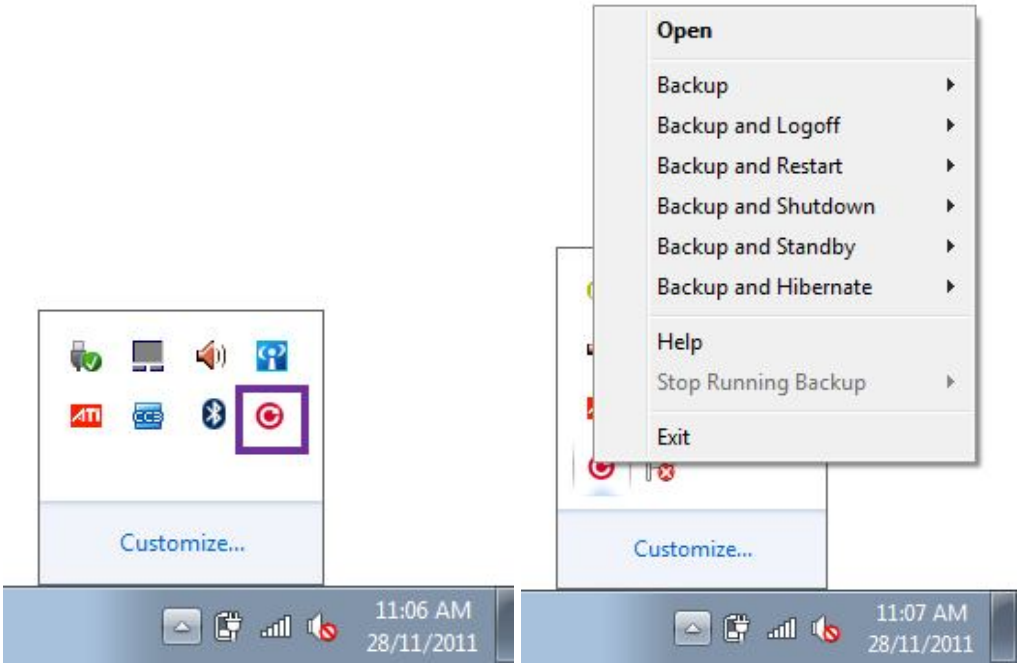
Quick Backup will back up your system by taking the following steps:

1. Before running any backup activities, Quick Backup will run all Pre-Commands of the backup set.
2. For each volume that needed to be backed up, Quick Backup will issue a system backup command to backup each volume to a ShadowProtect backup image file (*.spf and *.spi file) and save it in the temporary directory you specified.
3. After all images file have been spooled to the temporary directory, Quick Backup will run all Post-Commands of the backupset.
4. Upload all files copied to the temporary directory to Quick Backup Server.

12.3 How to backup system with ShadowProtect

Please follow the instructions below to backup your system with ShadowProtect with Quick Backup:

1. Open Quick Backup by right clicking Quick Backup icon available in the system tray and choose [Open].

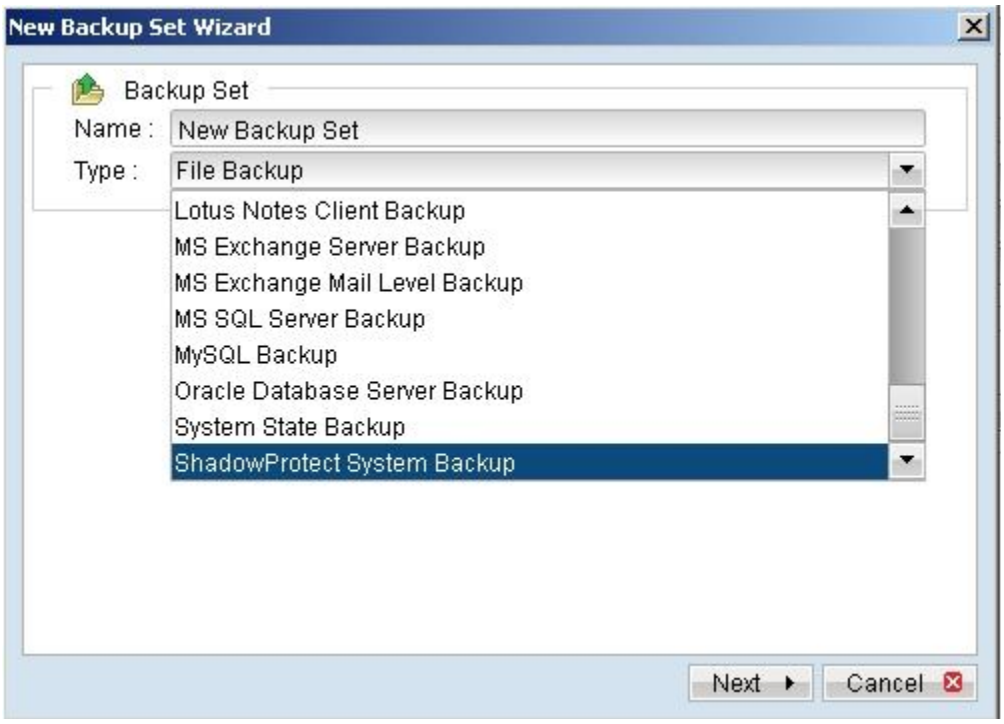


2. Create a backup set.

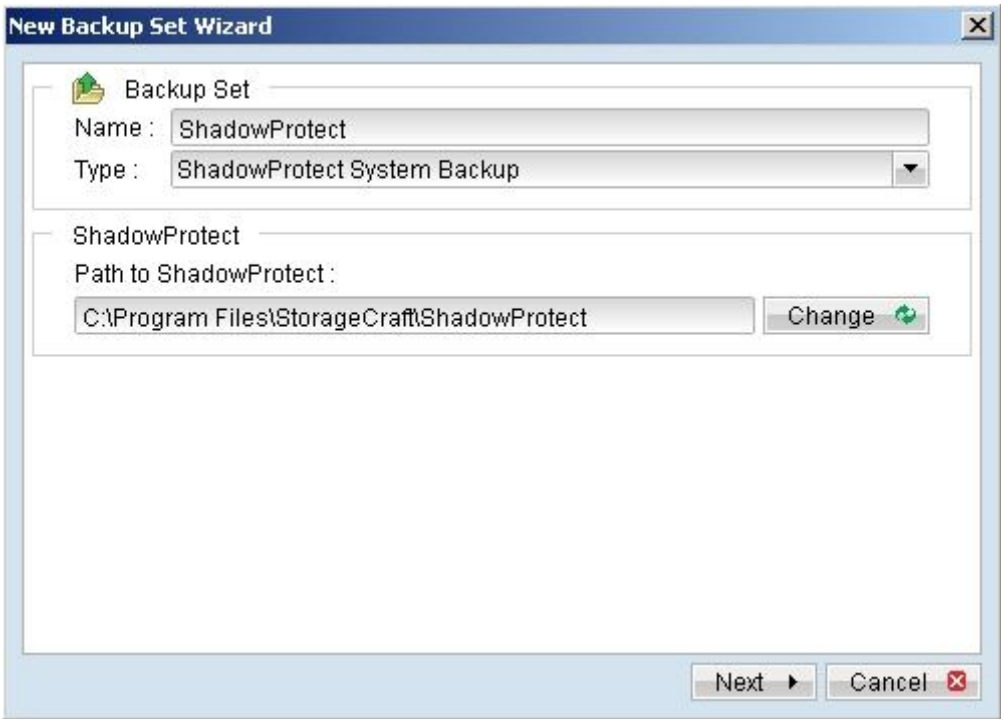
   i. To start setting up backup sets, click the button to open the [Backup Setting] dialog.

   ii. On the left panel, press the button to create a new backup set.

   iii. On the dialog, choose [ShadowProtect System Backup] as the [Type].

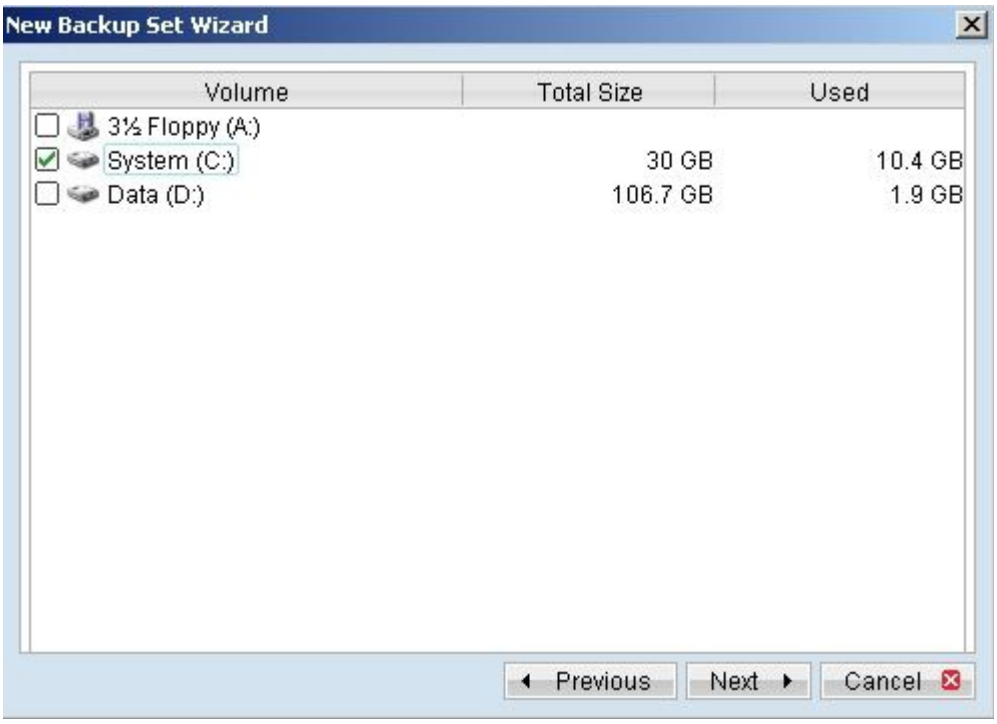


iv. Enter a name for your backup set.

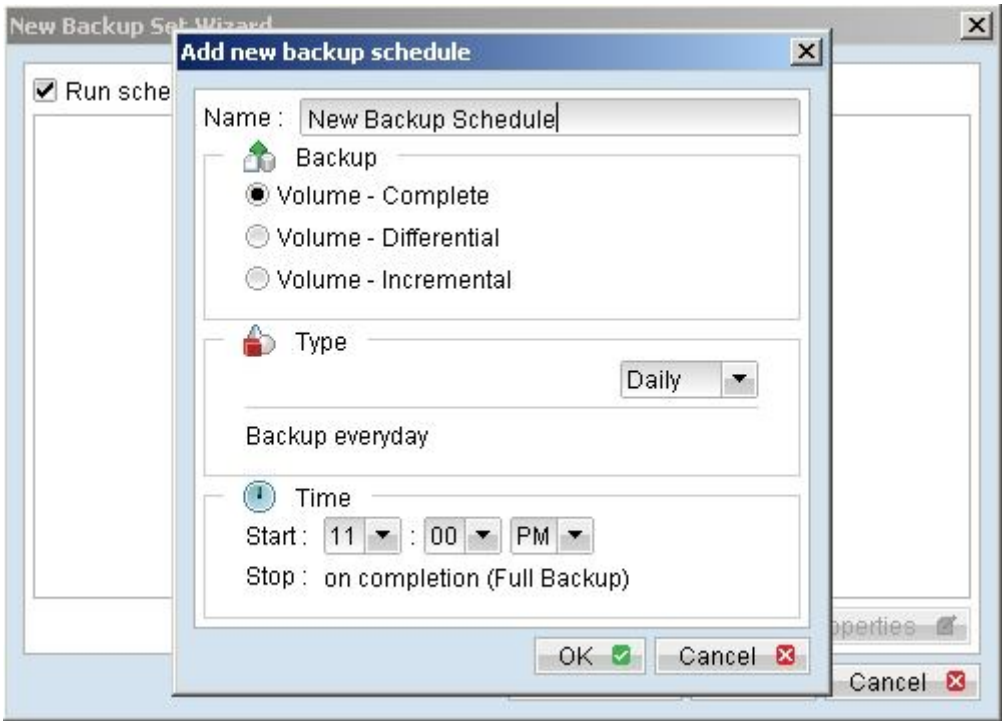


v. Enter the installation path of ShadowProtect.

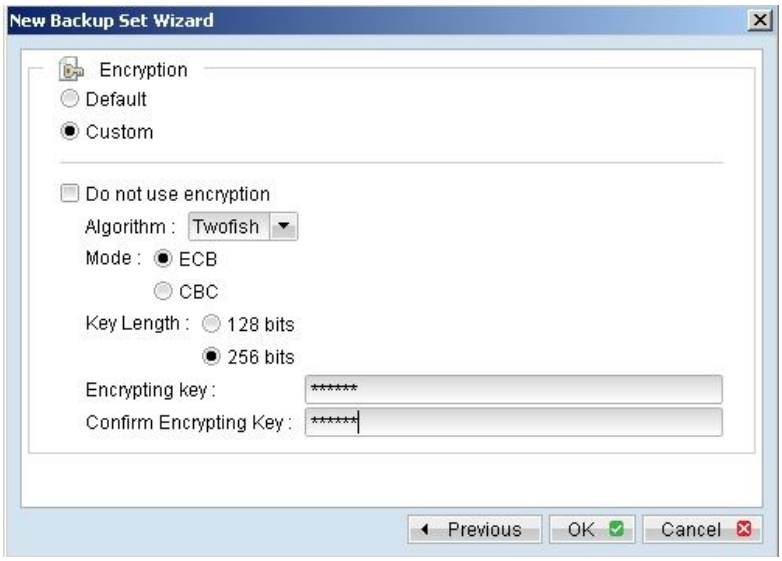
vi. Select the volume(s) you want to backup.



vii. Set the backup schedule.



viii. Set the encryption algorithm, encryption mode and encrypting key for this backup set.

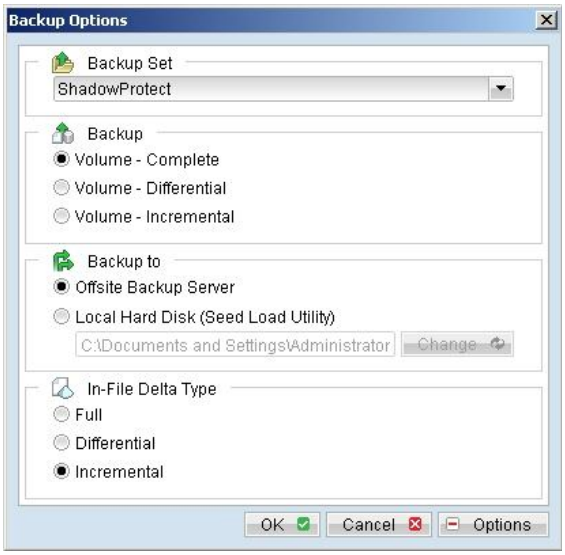


Important: If you have multiple disk partitions, please ensure that the temporary directory of the backup set is set to a disk volume which is different from the backup source. If you only have 1 disk partition, please delete the previous ShadowProtect backup file in your temporary directory before running a new backup. This will avoid a large backup image file to be created.

3. Run Backup.

i. Press the [Backup] button on the main page of Quick Backup dialog.

ii. Select the backup type (e.g. Complete, Differential, Incremental) you would like to perform. Select the backupset you want to run and select [Offsite Backup Server] to start backing up your files to Quick Backup Server. If applicable, you can also change the In-File Delta Type.



iii. Click [OK] to start backing up your files to Quick Backup Server.

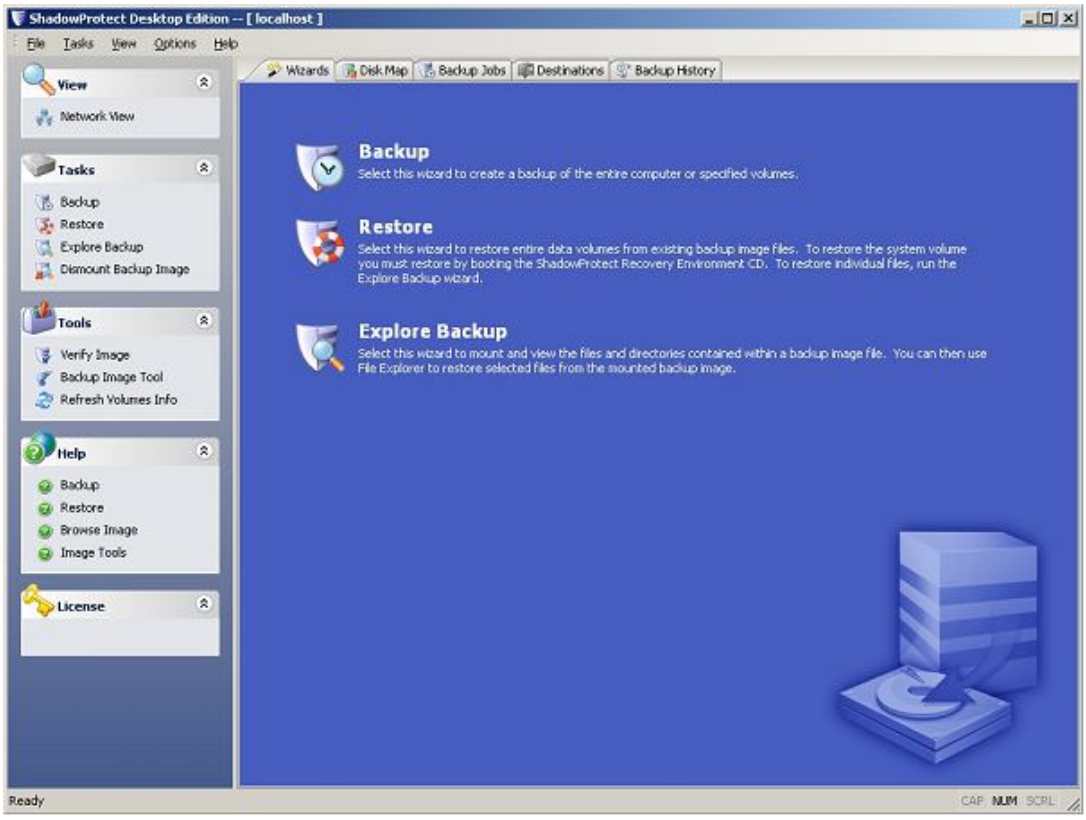
12.4 How to restore system with ShadowProtect

Please follow the instructions below to restore your system from Quick Backup Server.

1. Download the ShadowProtect backup file (*.spf, *.spi) from Quick Backup Server. Please refer to the Restoring Files section for information on how to download backup files from Quick Backup Server.

2. There are two methods that you can use to restore volumes. The first method is to boot to the StorageCraft Recovery Environment and perform the restore. This option must be used when restoring the system volume where the operating system resides. For more information about this method. The second method is to restore a volume, other than the system volume, which running inside Windows using Restore Volume Wizard. This method does not require the machine to be rebooted. To do so, please do the followings:

   i. Startup ShadowProtect or boot the StorageCraft Recovery Environment.


ShadowProtect Desktop Edition -- [localhost]
File Tasks View Options Help
View
Network View
Tasks
Backup
Restore
Explore Backup
Dismount Backup Image
Tools
Verify Image
Backup Image Tool
Refresh Volumes Info
Help
Backup
Restore
Browse Image
Image Tools
License
Wizards
Disk Map
Backup Jobs
Destinations
Backup History
Backup
Select this wizard to create a backup of the entire computer or specified volumes.
Restore
Select this wizard to restore entire data volumes from existing backup image files. To restore the system volume you must restore by booting the ShadowProtect Recovery Environment CD. To restore individual files, run the Explore Backup wizard.
Explore Backup
Select this wizard to mount and view the files and directories contained within a backup image file. You can then use File Explorer to restore selected files from the mounted backup image.
Ready
CAP NUM SCRL

   ii. Start Restore Wizard by clicking the [Restore] button in the left panel of the main screen or clicking on the Restore Wizard from the center panel of the main screen.

Restore
Welcome to the Restore Wizard!
This wizard will help you to restore entire data volumes from existing backup image files. To restore the system volume you must restore by booting the ShadowProtect Recovery Environment CD. To restore individual files, run the Explore Backup wizard.
Press Next to continue
< Back
Next >
Cancel

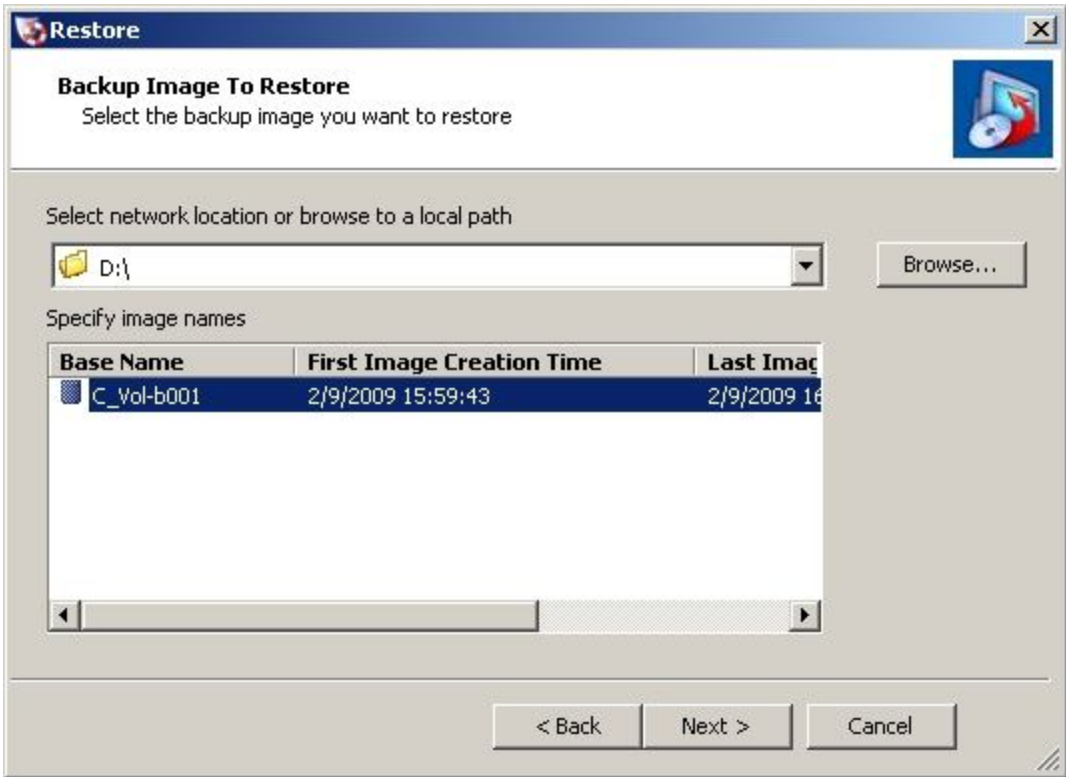
iii. Click [Next] to continue.

iv. This will bring up the Backup Image to Restore dialog screen. You will need to locate the image file you wish to restore from a destination location. These destination locations can be a local directory or network share.

- If the image file you wish to restore is located in a previously defined destination location. These destination locations can be a local directory or network share.
- If the image file you wish to restore is not located in a previously defined location, you will need to browse to the location of the image file you want to restore.

Note: To restore a backup image that is stored on a network share, you must have the proper credentials to access the file.

Click [Next] to continue.

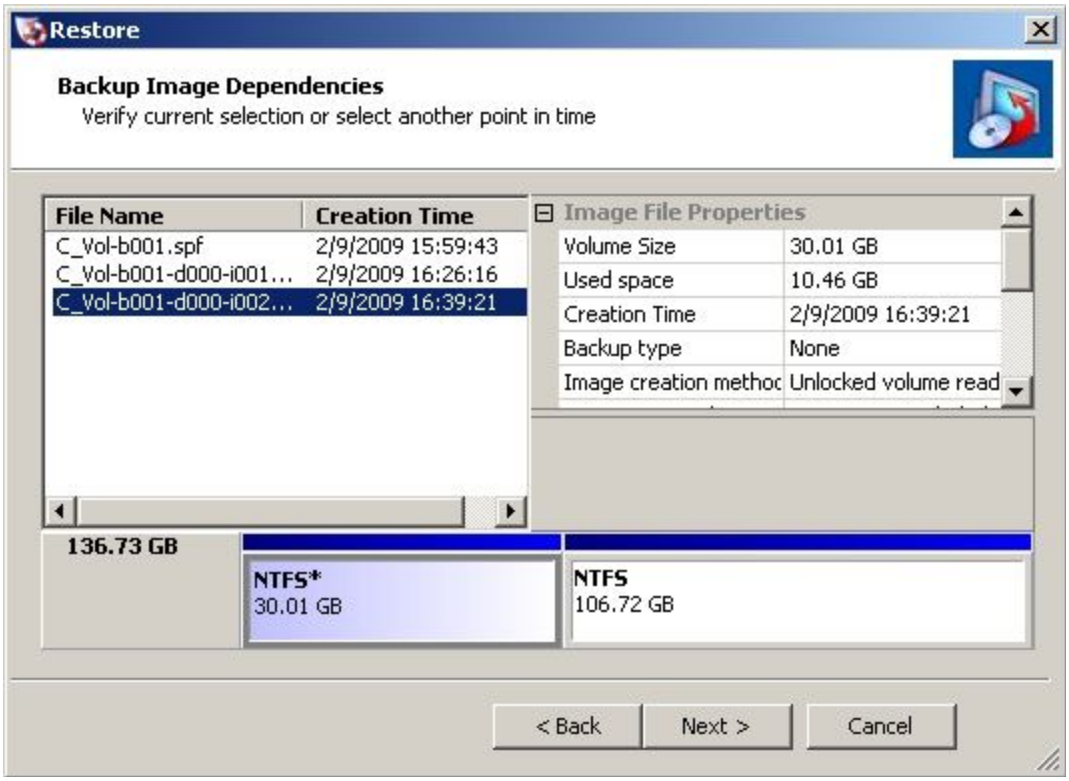


v. This will bring up the Backup Image Dependencies dialog screen. Here you will be provided with all the incremental backup image files associated with the full backup image file you selected. Select a backup image file to view its properties in the right side of the dialog. Image file properties include:

- Image File Properties – volume size, creation time, compression, password protection, comment.
- Original Partition Information – style, number, type, bootable option, starting offset and length.
- Disk Information – disk geometry, disk size and number of the first track sectors. You can also view the disk layout graphically at the bottom of the screen. This represents what the disk looked like at the time of backup.
- Originating machine – the operating system version, the machine name, MAC address and the engine version of ShadowProtect used to create the image file.

By viewing the properties, particularly the information in the image file properties, you will be able to select the backup image file you wish to restore. You can change your selection and review the new selection's image file properties by highlighting the image file in the left side of the dialog screen.

Click the [Next] to continue.



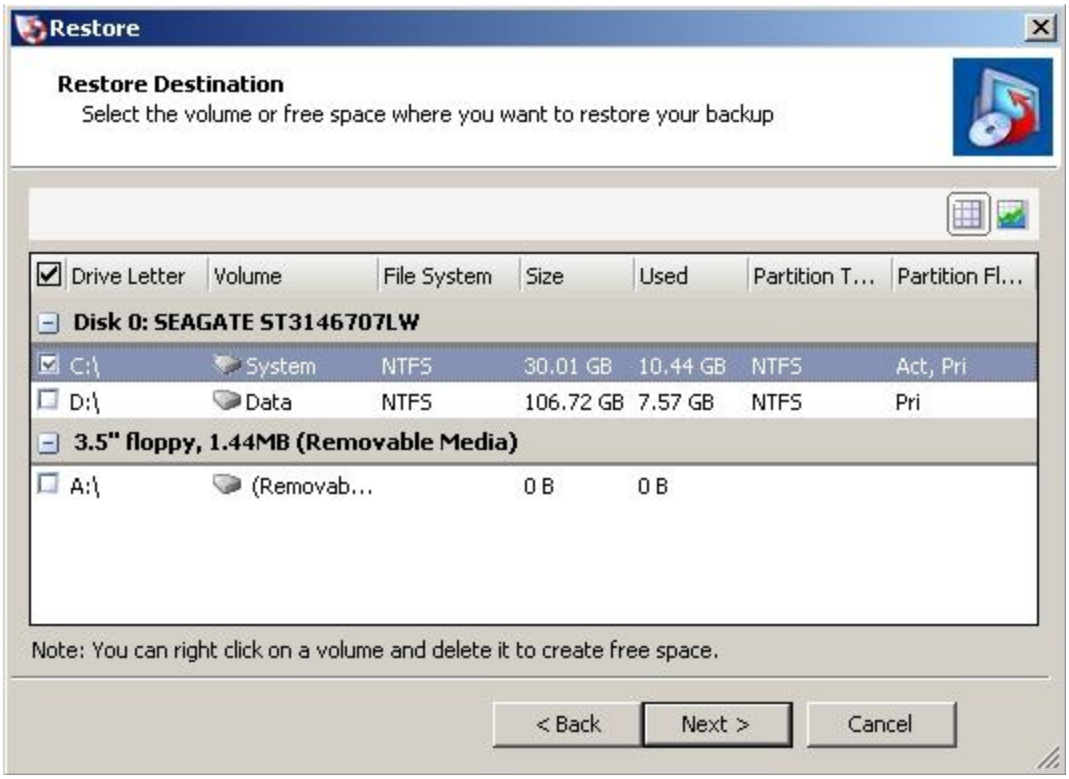
vi. This will bring up the Restore Destination dialog screen. Select the location where you want to restore the backup image. You may also right click on a volume and you will have the following options:

- Delete Volume – This will delete a volume. The deleted volume will become unassigned space on the disk that can be repartition.
- Set Active – This will set the volume active. Only one partition may be designated as active. By setting a volume active, the computer will boot to the volume.
- Create an exact primary partition – Allows you to define and create a primary partition on the disk. You cannot create more than four (4) primary partitions on the same disk.
- Create extended partition – Allows you to extend a partition and then subdivide this partition in to one or more logical partitions.

Note: Restoring a backup image to a volume overwrites all data currently on the volume.

Note: You must have enough space to restore the backup image. For example, you cannot restore a 4GB backup file with only 1GB of free space.

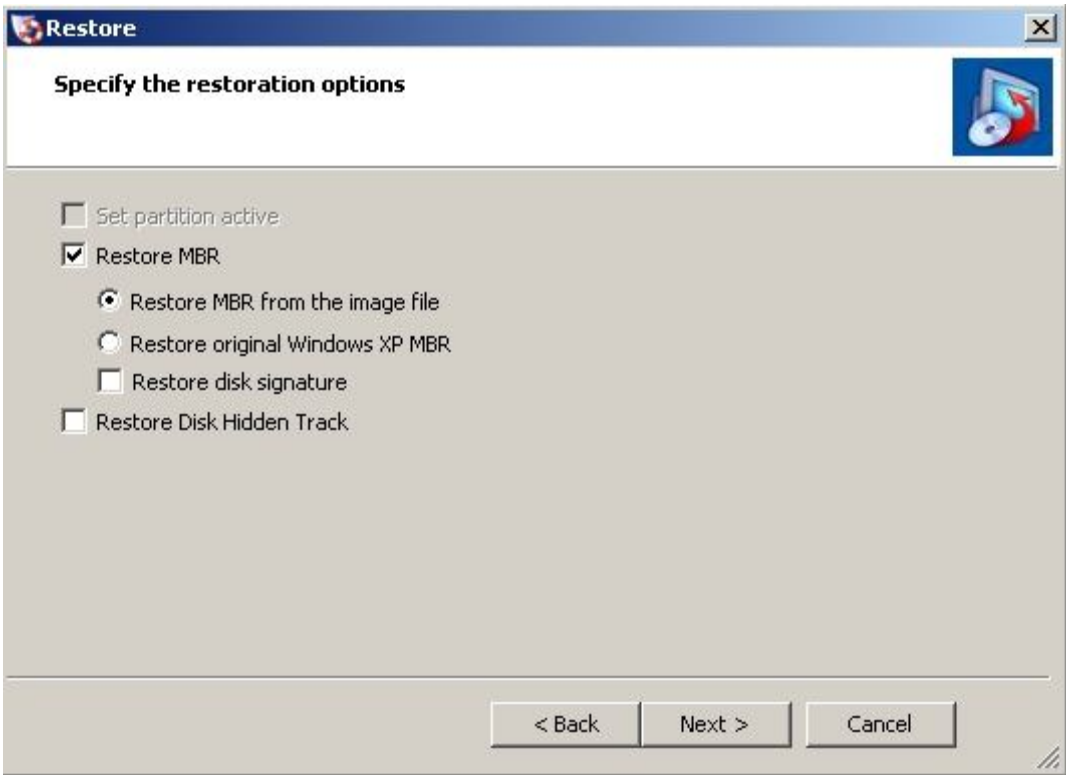
Click [Next] to continue.


Restore
Restore Destination
Select the volume or free space where you want to restore your backup
Drive Letter
Volume
File System
Size
Used
Partition T...
Partition Fl...
Disk 0: SEAGATE ST3146707LW
C:\ System NTFS 30.01 GB 10.44 GB NTFS Act, Pri
D:\ Data NTFS 106.72 GB 7.57 GB NTFS Pri
3.5" floppy, 1.44MB (Removable Media)
A:\ (Removab... 0 B 0 B
Note: You can right click on a volume and delete it to create free space.
< Back
Next >
Cancel

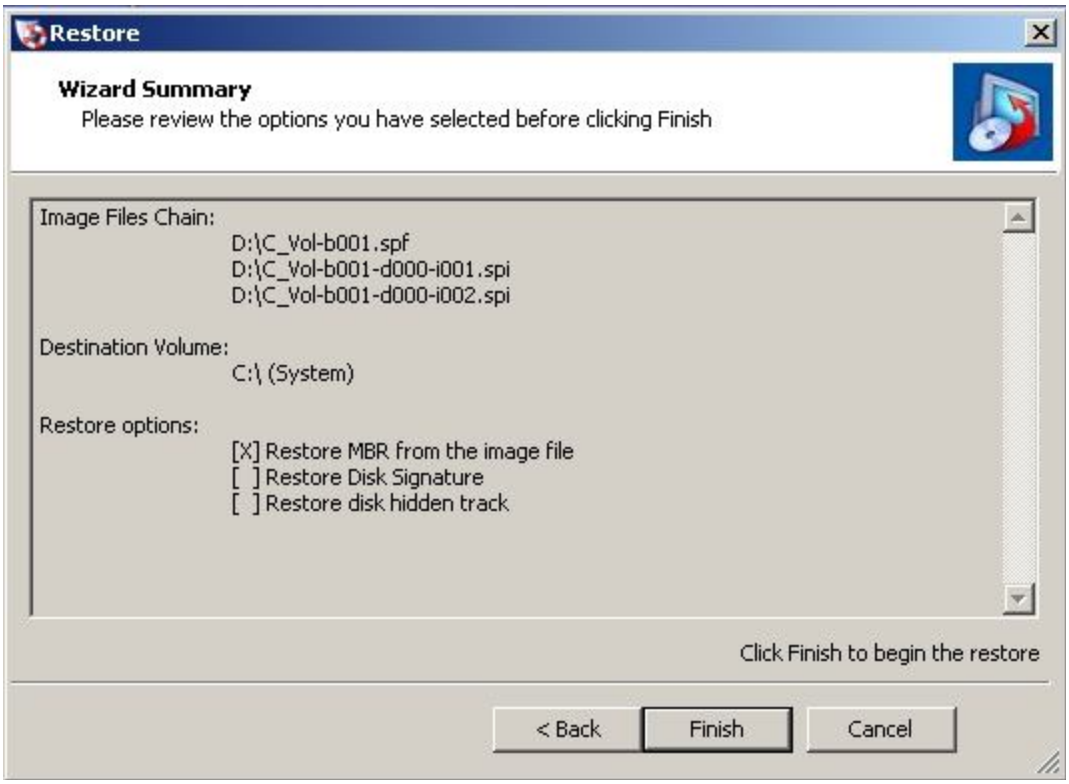
vii. This will bring up the [Specify the Restoration Options] dialog screen. All of these options are important where restoring the system volume on a computer.

- Set Partition Active – This will make the restored drive the active partition (the drive that the machine boots from).
- Restore MBR – Restore the master boot record. The master boot record is contained in the first sector of the first physical hard drive. The MBR consists of a master boot program and a partition table that describes the disk partitions. The master boot program looks at the partition table to see which primary partition is active. It then starts the boot program from the boot sector of the active partition. You can restore the MBR from the image file that was saved with the backup image or you can restore an original Windows MBR.
- Restore disk signature – Restores the original physical disk signature of the hard drive. Disk signatures are included in Windows Server 2003, Windows 2000 Advanced Server, and Windows NT Server 4.0 Enterprise Edition(SP3 and later) and are necessary before the hard drive can be used.
- Restore Disk Hidden Track – this will restore the first 63 sectors of a drive. Some boot loaded applications required this for the system to boot.

Click [Next] to continue.



viii. This will bring up the Wizard Summary. Review the Restore Wizard Summary and click [Finish] to start restoring the volume.



ix. You can review the progress of restoring the volume by clicking on the [Volume Restore] tab associated with the restore job.

3. All volume(s) are restored successfully.

13 Backup / Restore VMware Virtual Machines

This chapter describes how to backup and restore virtual machines running on VMware ESX, ESXi Server or VMware Server 2.0.

13.1 Backup virtual machines running on VMware ESXi / ESX Server

13.1.1 Supported versions

The VMware VM backup module is supported for the following VMware ESXi / ESX versions:

- VMware ESXi 3.5
- VMware ESXi 4.0
- VMware ESXi 4.1
- VMware ESXi 5.0

- VMware ESX 3.5
- VMware ESX 4.0
- VMware ESX 4.1

13.1.2 Requirements and Recommendations

A dedicated physical machine – the backup client computer - is used for backup of your virtual machines.

Please ensure that the following requirements or recommendations are met by the **backup client computer**:

1. The backup client computer is running on:

   - Windows
   - Linux
   - Mac OS X

2. Quick Backup version 6.7 or above is installed on the backup client computer.

3. The following TCP ports must be opened on the backup client computer:

   - Port 22
   - Port 80 and 443

4. For better performance, Quick Backup is recommended to be installed on a 64 bit computer, with multiple CPUs and cores.

5. For backup client machine running on Linux, GUI environment must be installed (e.g. GOME or KDE).

6. Consider increasing the JVM (Java Virtual Machine) memory allocation to improve performance of the backup operation.

7. It is recommended that the temporary directory have disk space of at least 50% of the largest sized virtual machine to be backed up.

8. It is recommended that the temporary directory be configured on a local drive.

9. It is recommended that the temporary directory is not configured on the same partition which the operating system is installed on.

Please ensure that the following requirements are met by the **hypervisor**:

1. SSH must be enabled on the hypervisor.

2. The root account **must be** enabled.

   Quick Backup ESX / ESXi backup set requires the root account for backup and restore.

3. The following TCP ports must be opened on the hypervisor:

   - Port 22
   - Port 80 and 443

4. Snapshot of virtual machines selected for backup are stream from the hypervisor (datastore of the corresponding VM) to the Quick Backup Server server.

5. It is recommended that the datastore have disk space of the largest sized virtual machine to be backed up.

13.1.3 Limitation

The following are limitations of the VMware VM backup module:

1. Existing snapshot of all virtual machines (selected for backup) are removed during the backup process.

2. Independent Disk of VMware is not supported. For virtual machines with Independent Disks, those disks will not be backed up.

3. VMware ESX or ESXi Server with Raw Device Mapping (RDM) is not supported. Snapshots are not available when the RDM is used in physical compatibility mode.

4. VMware ESX Server Cluster (Resource Pool) is not supported.

13.1.4 Overview

The following steps take place when a virtual machine backup is performed with Quick Backup:

1. Connection from the backup client to the backup server is established.
2. Download the server file list from the backup server.
3. Connection from the backup client to the hypervisor is established.
4. Commands are issued to the hypervisor to remove existing snapshot of virtual machine (if necessary).
5. Commands are issued to the hypervisor to create snapshot of the virtual machine.
6. Server and local file lists are compared to determine which file will be uploaded.
7. Delta file is generated for modified file (if necessary).
8. Data are encrypted, compressed, and streamed to the backup server.
9. Commands are issued to the hypervisor to remove snapshot created.
10. Steps 3 to 8 are performed for each virtual machine selected for backup.
11. Backup completed successfully.

Important:

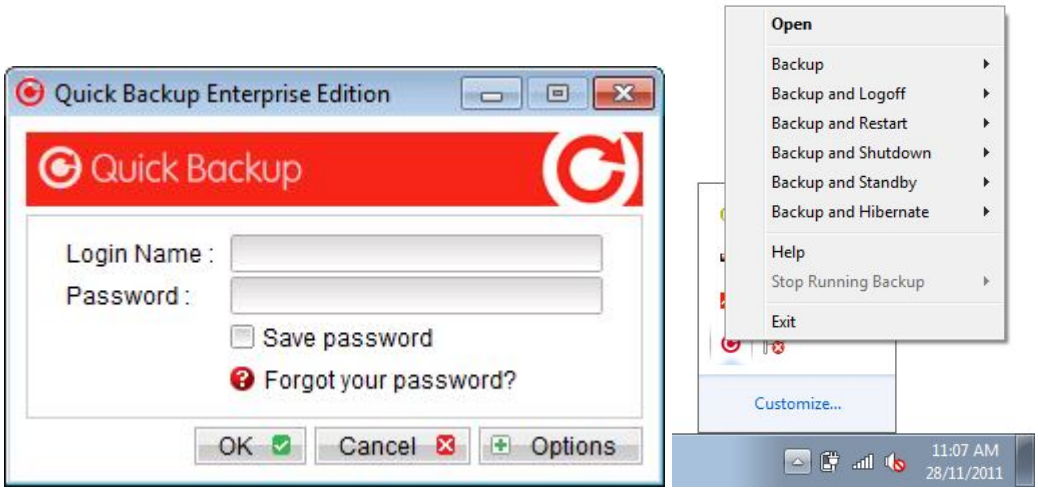
- Existing snapshot of all virtual machines selected will be **deleted** before they are backed up.
- For hypervisor with Raw Device Mapping (RDM), snapshots are not available when the RDM is used in physical compatibility mode.
- For virtual machines with Independent Disks (designed not to allow snapshot), those disks **will not** be backed up.

13.1.5 How to backup virtual machines on VMware ESXi / ESX Server

Refer to the follow instructions to backup virtual machines running on VMware ESXi or ESX Server:

1. Login to the backup application's user interface.

For backup client computer on Windows, double-click on the Quick Backup desktop icon or right-click on the system tray icon:

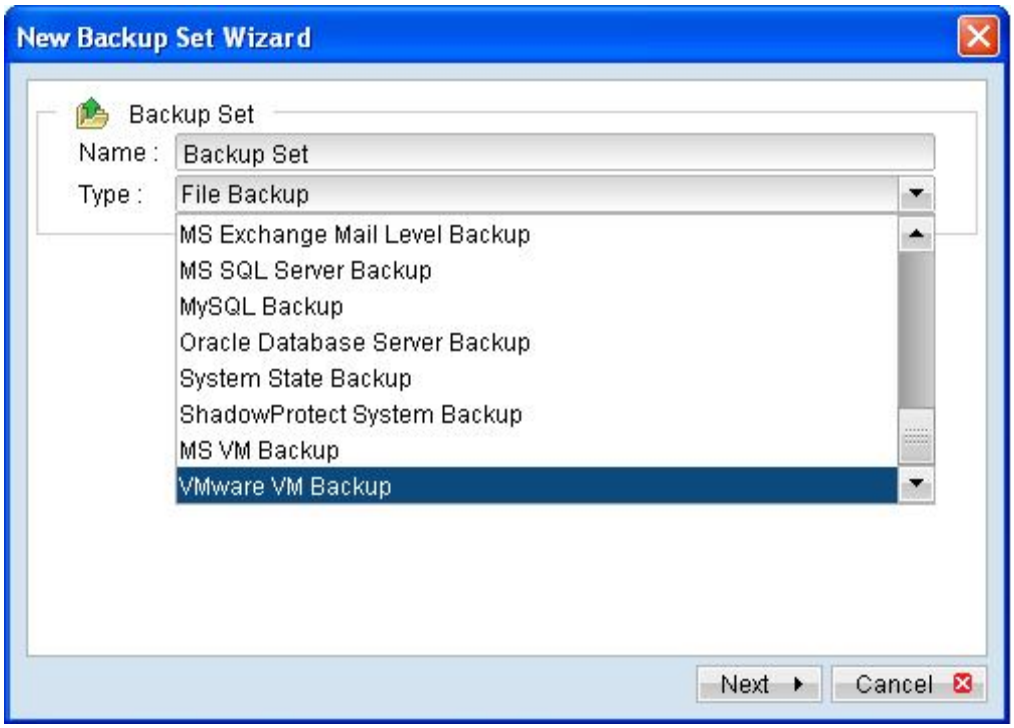


For backup client computer on Mac OS X, double-click on the Quick Backup desktop icon.

For VMware Server installation on Linux, enter the following command to start the Quick Backup graphical user interface:

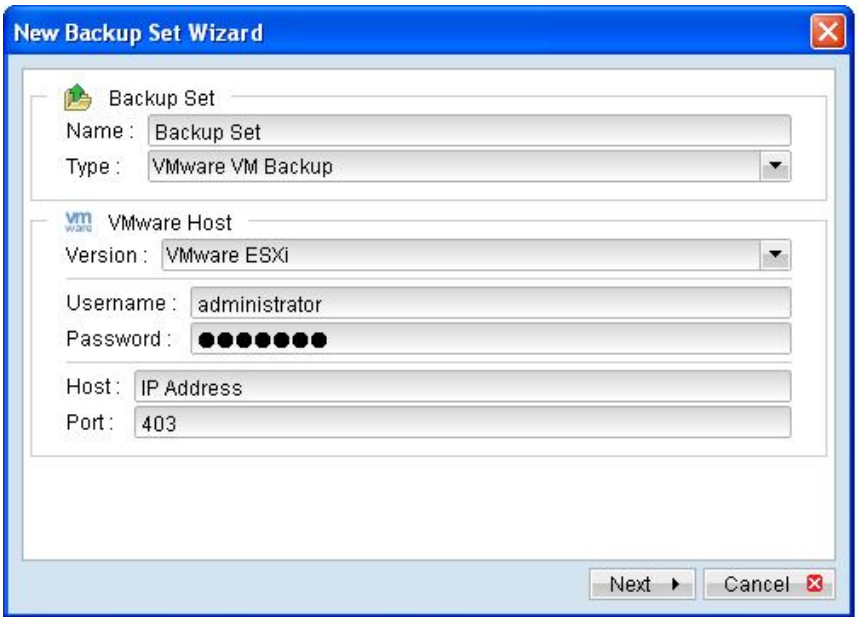
```
# sh /usr/local/obm/bin/RunOBC.sh &
```

2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.



3. Create a VMware VM Backup set by selecting [VMware VM Backup] from the backup set type dropdown menu.

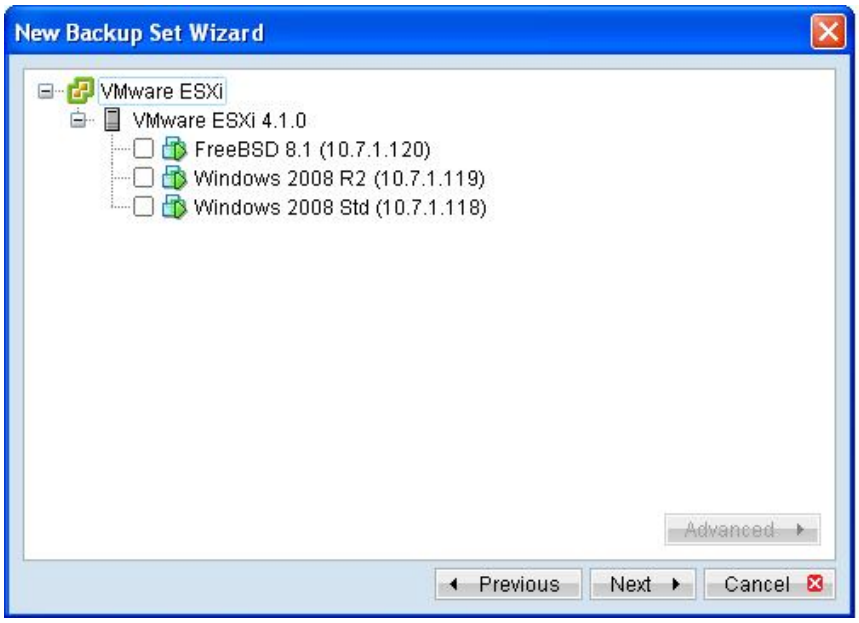
4. Enter the corresponding information required:



Menu Items	Description
Name	Enter a backup set name of your choice.
Type	Select backup set type [VMware VM Backup].
VMware Host Version	Select version [VMware ESXi] or [VMware ESX] according to your setup.
Username	The username **must be** root
Password	Enter the password for the root account.
Host	Enter the IP address or hostname of your hypervisor.
Port	Enter 80 for connection via HTTP protocol or 443 for HTTPS protocol.

5. Select [Next] to proceed.

6. Select the corresponding virtual machines for backup.



7. Configure a backup schedule for unattended backups.

8. Select an encryption setting for your backup set.

9. Press the [OK] button to complete the configuration of backup set.

10. Scheduled backup will run automatically if you leave your computer on.

11. To perform a backup immediately, click [Backup] button on the left panel.

13.1.6 How to restore virtual machines on VMware ESXi / ESX Server

For restore to the original hypervisor, the virtual machine will be restored under the following conditions:

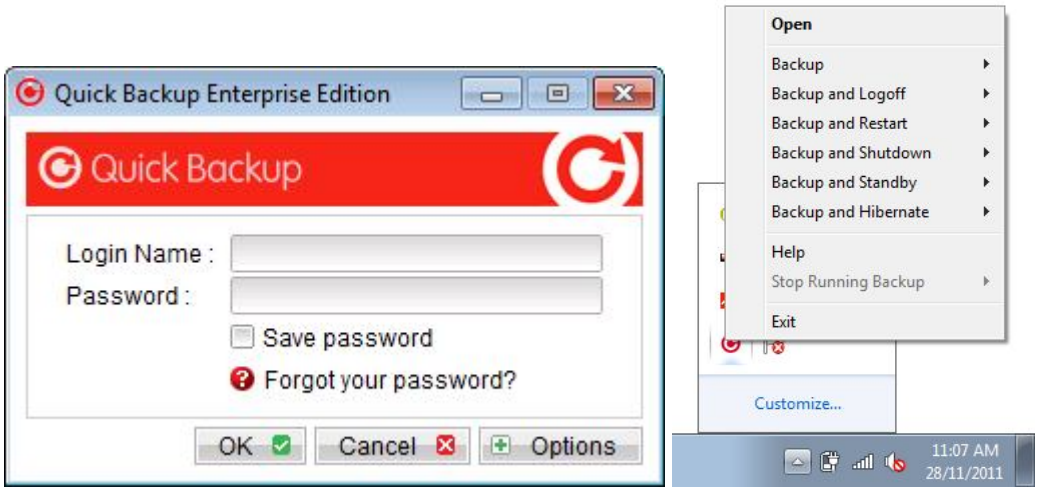
- If the virtual machine to be restored no longer exist on the original hypervisor. The VM will be restored as a new virtual machine.
- If the virtual machine to be restored still exist on the original hypervisor. The existing VM will be replaced by the backed up version.

Refer to the follow instructions to restore virtual machines running on VMware ESXi or ESX Server.

Restoring to the original hypervisor:

1. Login to the backup application's user interface.

For backup client computer on Windows, double-click on the Quick Backup desktop icon or right-click on the system tray icon:

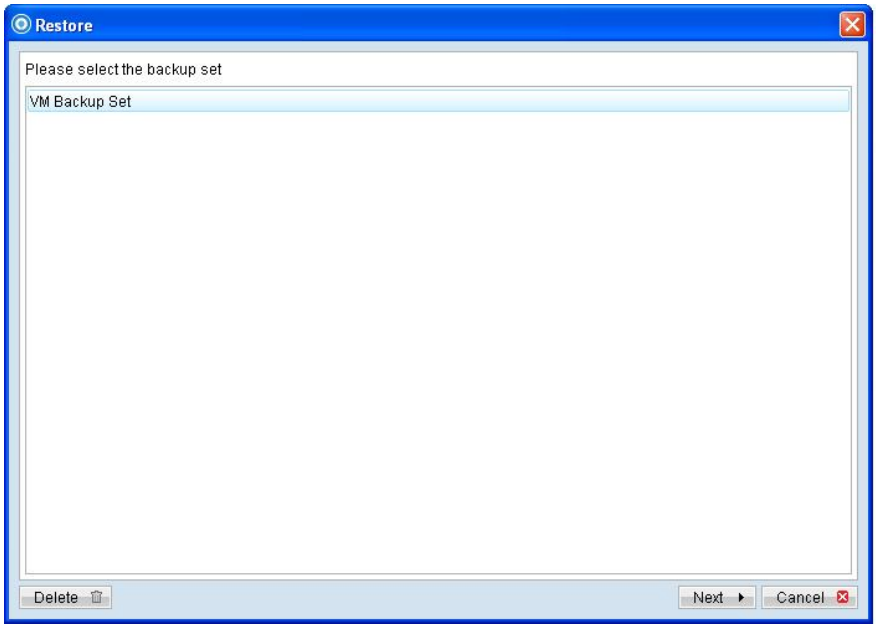


For backup client computer on Mac OS X, double-click on the Quick Backup desktop icon.

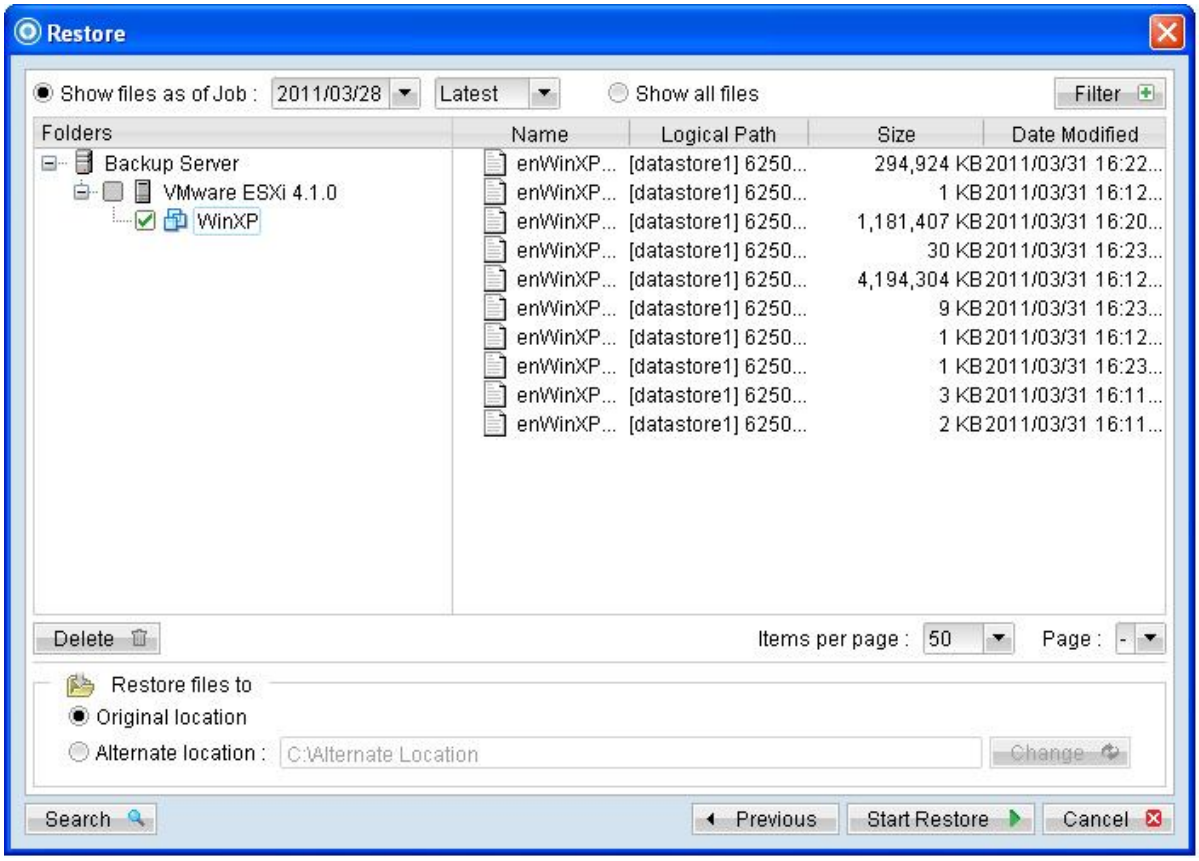
For VMware Server installation on Linux, enter the following command to start the Quick Backup graphical user interface:

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

2. Select the [Restore] button and the corresponding backup set.

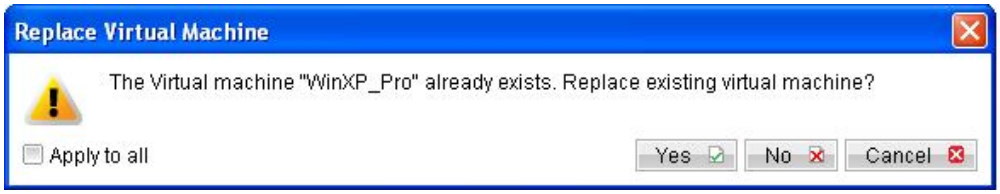


3. Select the virtual machines to be restored and choose [Original Location] for restore files to.



4. Click the [Start Restore] button to begin the restore process.

5. User will be prompted if a virtual machine selected to be restored exist on the hypervisor.

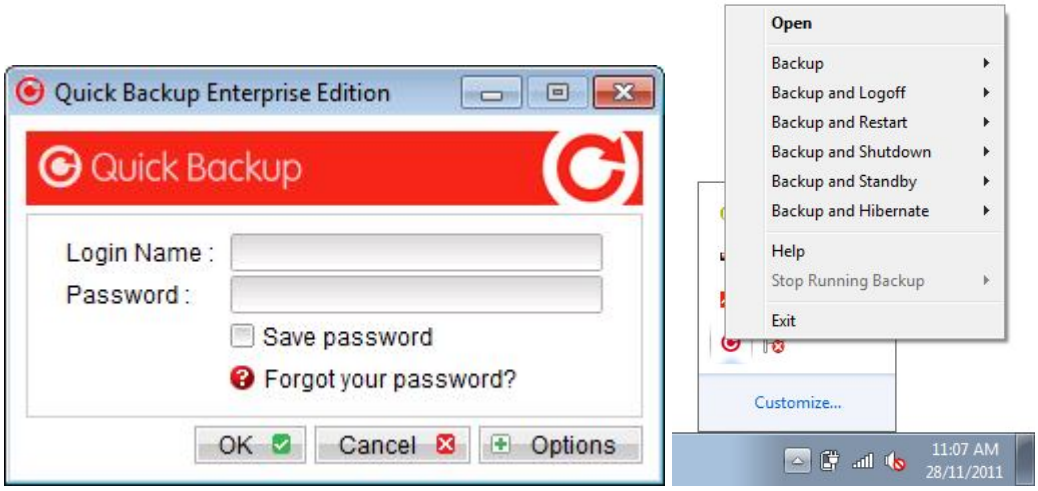


6. When the restore process is completed, the virtual machines will be restored to the original hypervisor.

Restoring to another hypervisor:

1. Login to the backup application's user interface.

For backup client computer on Windows, double-click on the Quick Backup desktop icon or right-click on the system tray icon

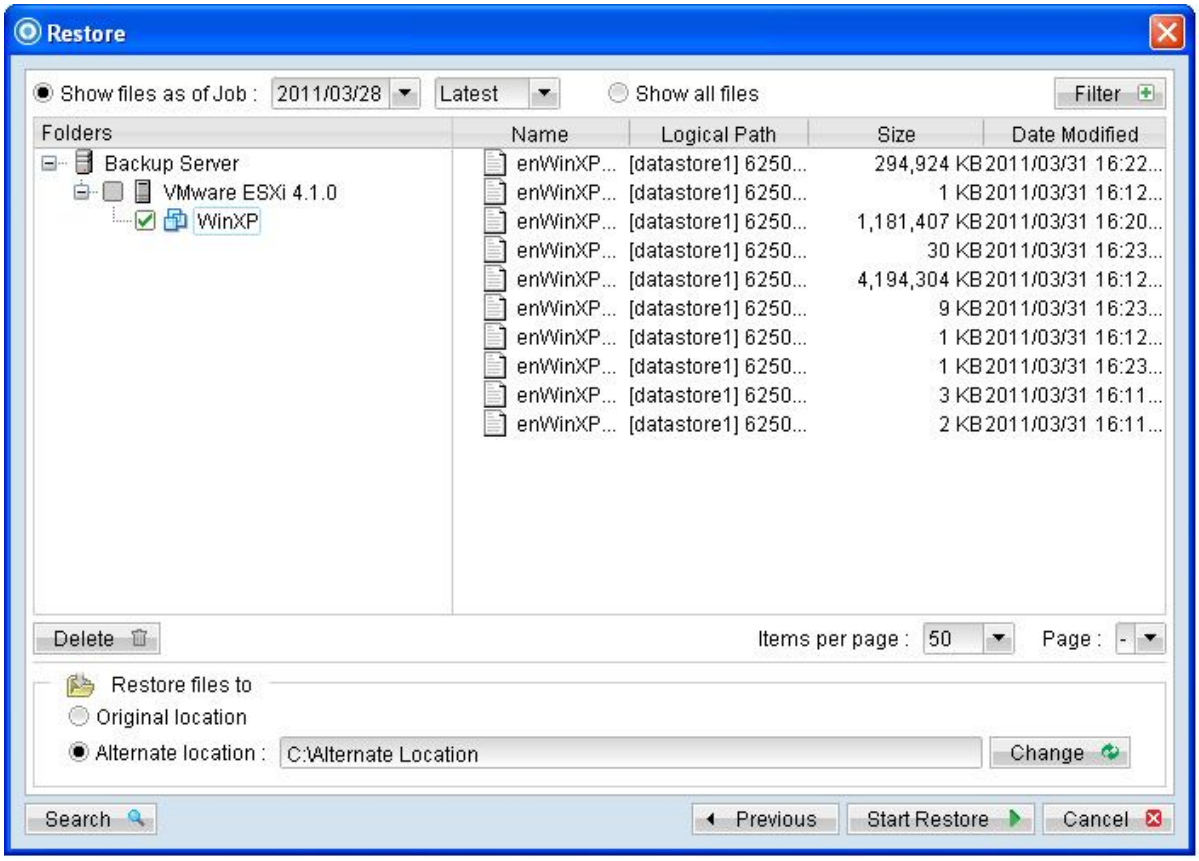


For backup client computer on Mac OS X, double-click on the Quick Backup desktop icon.

For VMware Server installation on Linux, enter the following command to start the Quick Backup graphical user interface:

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

2. Select the [Restore] button and the corresponding backup set.



3. Select the virtual machines to be restored and choose [Alternate location] for restore files to.

4. Click on the [Change] button and browse to the directory path which you would like to restore the data to.

5. Click the [Start Restore] button to begin the restore process.

6. When the restore process is completed, data of the selected virtual machines will be restored to the specific location.

7. Re-register the virtual machines on the new hypervisor. Please consult your VMware hypervisor administrator for more details.

13.2 Backup virtual machines running on VMware Server

13.2.1 Supported versions

The VMware VM backup module is supported for the following VMware Server versions:

- VMware Server 2.x

13.2.2 Requirements and Recommendations

Please ensure that the following requirements are met:

1. Quick Backup version 6.7 or above is installed on the VMware Server.

   Note:
   Resource allocation for both VM hosting and backup operation **must be** taken into consideration.

2. Quick Backup **must be** installed on the hypervisor.

3. For backup of virtual machines with multiple snapshot trees, a valid VMware Foundation License must be applied on the hypervisor.

4. **For VMware Server installation on Linux:**

   - The root account must be enabled.
   - GUI environment must be installed on the hypervisor (e.g. GOME or KDE).

5. The following TCP ports must be opened on the hypervisor:

   - Port 902
   - Port 8222
   - Port 8333

6. Consider increasing the JVM (Java Virtual Machine) memory allocation to improve performance of the backup operation.

7. Snapshot of virtual machines selected for backup are stream from the hypervisor (datastore of the corresponding VM) to the Quick Backup Server server.

8. It is recommended that the datastore have disk space of the largest sized virtual machine to be backed up.

9. It is recommended that the temporary directory have disk space of at least 50% of the largest sized virtual machine to be backed up.

10. It is recommended that the temporary directory be configured on a local drive.

11. It is recommended that the temporary directory is not configured on the same partition which the operating system is installed on.

13.2.3 Limitation

The following are limitations of the VMware VM backup module:

1. Existing snapshot of all virtual machines (selected for backup) are removed before the backup process begin.

2. Independent Disk of VMware is not supported. For virtual machines with Independent Disks, those disks will not be backed up.

13.2.4 Overview

The following steps take place when a virtual machine backup is performed with Quick Backup:

1. Connection from the backup client to the backup server is established.

2. Download the server file list from the backup server.

3. Commands are issued to the hypervisor to remove existing snapshot of the virtual machine (if necessary).

4. Commands are issued to the hypervisor to create snapshot of the virtual machine.

5. Server and local file lists are compared to determine which file will be uploaded.

6. Delta file is generated for modified file (if necessary).

7. Data are encrypted, compressed, and streamed to the backup server.

8. Commands are issued to the hypervisor to remove snapshot created.

9. Steps 3 to 8 are performed for each virtual machine selected for backup.

10. Backup completed successfully.

Important:

- Existing snapshot of all virtual machines selected will be **deleted** before they are backed up.

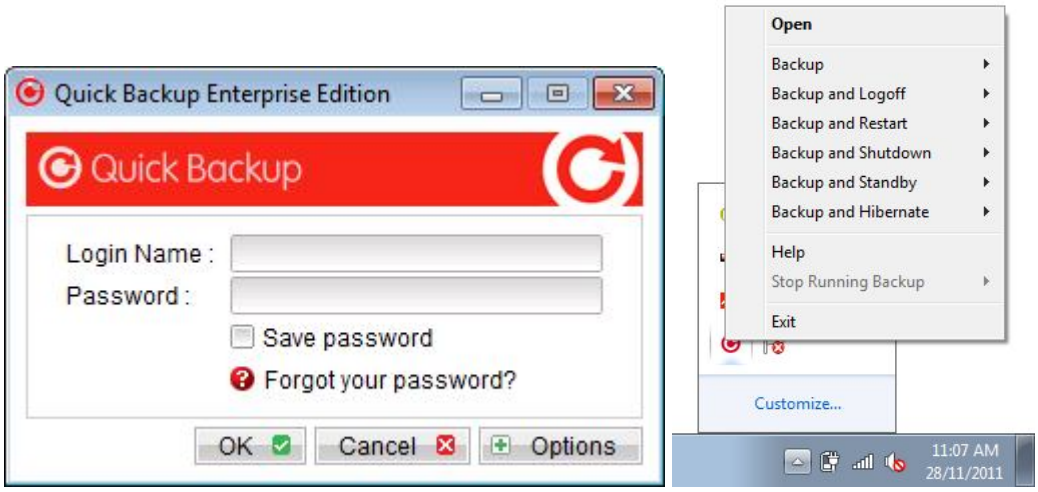
- For virtual machines with Independent Disks (designed not to allow snapshot), those disks **will not** be backed up.

13.2.5 How to backup virtual machines on VMware Server

Refer to the follow instructions to backup virtual machines running on VMware Server:

1. Login to the backup application’s user interface.

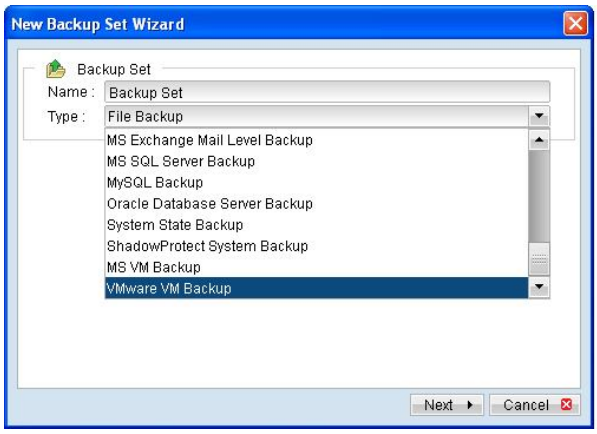
For VMware Server installation on Windows, double-click on the Quick Backup desktop icon or right-click on the system tray icon:

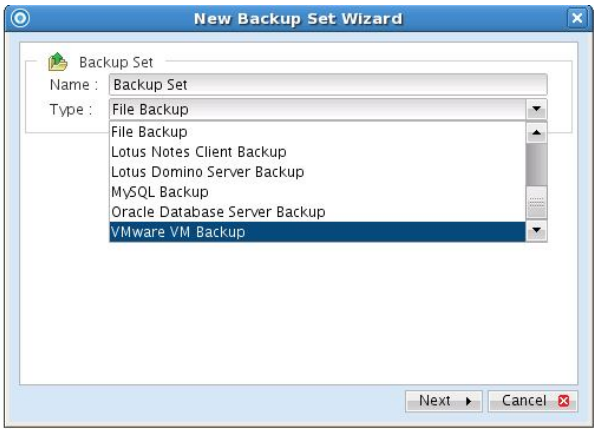


For VMware Server installation on Linux, enter the following command to start the Quick Backup graphical user interface:

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

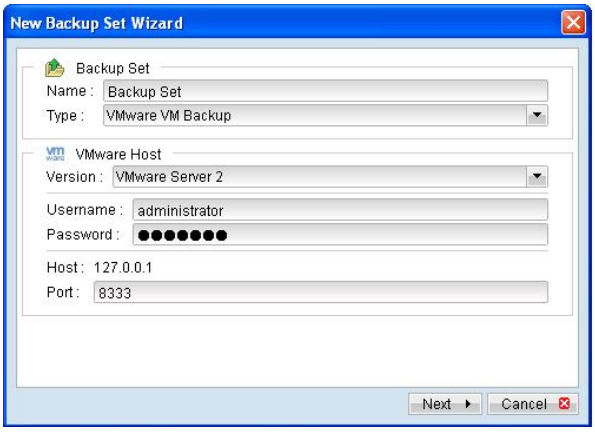
2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

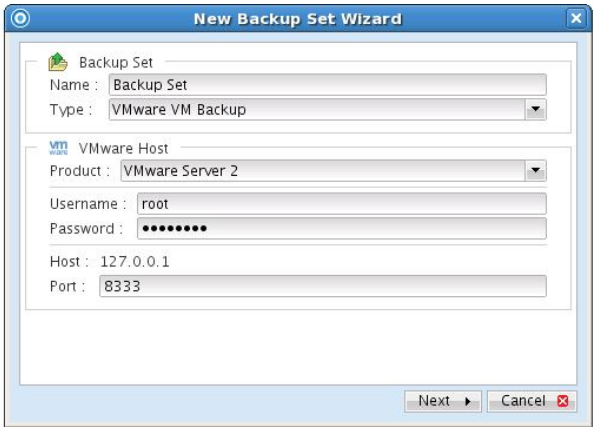




3. Create a VMware VM Backup set by selecting [VMware VM Backup] from the backup set type dropdown menu.

4. Enter the corresponding information required:

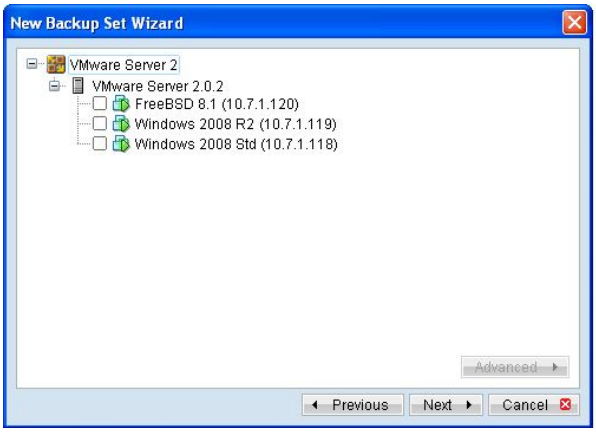


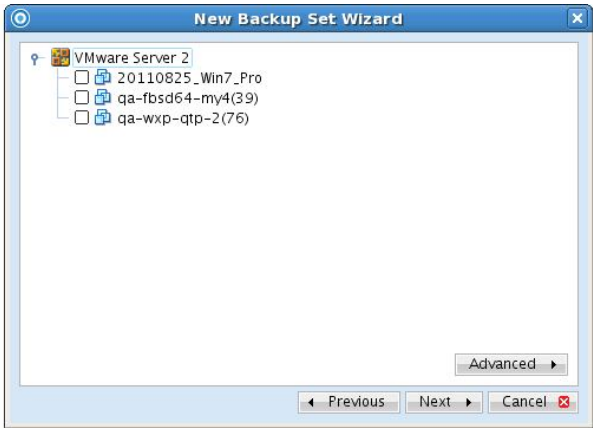


Menu Items	Description
Name	Enter a backup set name of your choice.
Type	Select backup set type [VMware VM Backup].
VMware Host Version	Select host version, for example [VMware Server 2].
Username	Enter the username of the hypervisor administrator.
Password	Enter the password of the hypervisor administrator.
Host	Host will be default to 127.0.0.1 (localhost), as Quick Backup must be installed on the hypervisor.
Port	Enter 8222 for connection via HTTP protocol or 8333 for HTTPS protocol.

5. Select [Next] to proceed.

6. Select the corresponding virtual machines for backup.





7. Configure a backup schedule for unattended backups.

8. Select an encryption setting for your backup set.

9. Press the [OK] button to complete the configuration of backup set.

10. Scheduled backup will run automatically if you leave your computer on.
11. To perform a backup immediately, click [Backup] button on the left panel.

13.2.6 How to restore virtual machines on VMware Server

For restore to the original hypervisor, the virtual machine will be restored under the following conditions:

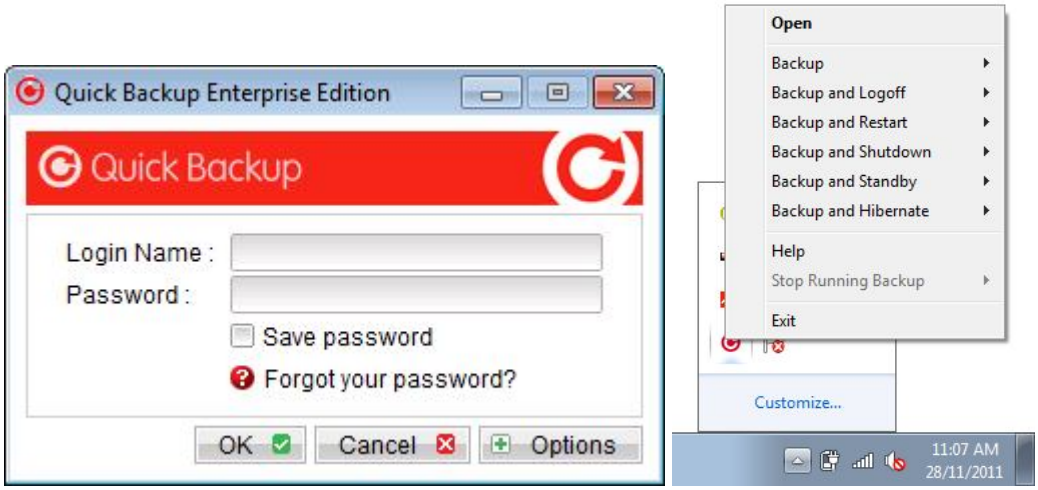
- If the virtual machine to be restored no longer exist on the original hypervisor. The VM will be restored as a new virtual machine.
- If the virtual machine to be restored still exist on the original hypervisor. The existing VM will be replaced by the backed up version.

Refer to the follow instructions to restore virtual machines running on VMware Server.

Restoring to the original hypervisor:

1. Login to the backup application's user interface.

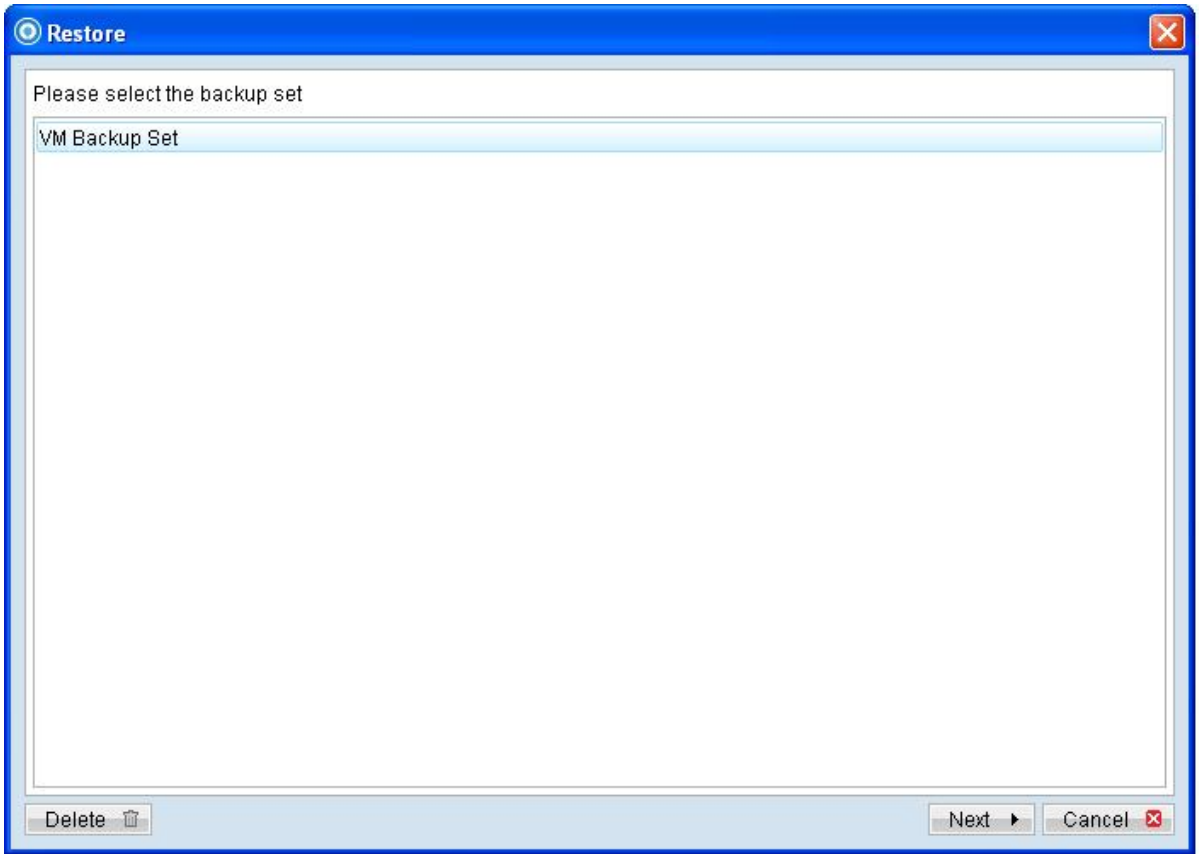
For VMware Server installation on Windows, double-click on the Quick Backup desktop icon or right-click on the system tray icon:



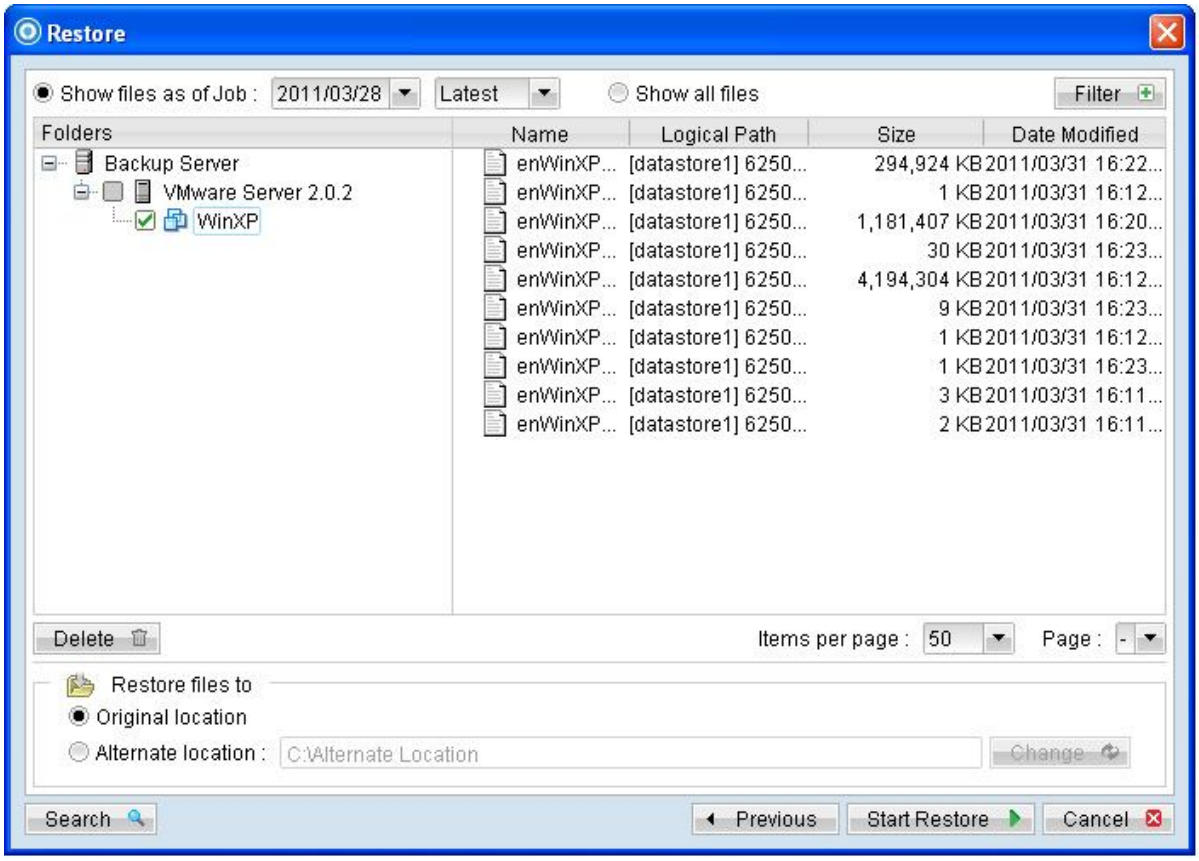
For VMware Server installation on Linux, enter the following command to start the Quick Backup graphical user interface:

```
# sh /usr/local/obm/bin/RunOBC.sh &
```

2. Select the [Restore] button and the corresponding backup set.



3. Select the virtual machines to be restored and choose [Original Location] for restore files to.


Restore
Show files as of Job : 2011/03/28 Latest Show all files Filter
Folders
Backup Server
VMware Server 2.0.2
WinXP
Name Logical Path Size Date Modified
enWinXP... [datastore1] 6250... 294,924 KB 2011/03/31 16:22...
enWinXP... [datastore1] 6250... 1 KB 2011/03/31 16:12...
enWinXP... [datastore1] 6250... 1,181,407 KB 2011/03/31 16:20...
enWinXP... [datastore1] 6250... 30 KB 2011/03/31 16:23...
enWinXP... [datastore1] 6250... 4,194,304 KB 2011/03/31 16:12...
enWinXP... [datastore1] 6250... 9 KB 2011/03/31 16:23...
enWinXP... [datastore1] 6250... 1 KB 2011/03/31 16:12...
enWinXP... [datastore1] 6250... 1 KB 2011/03/31 16:23...
enWinXP... [datastore1] 6250... 3 KB 2011/03/31 16:11...
enWinXP... [datastore1] 6250... 2 KB 2011/03/31 16:11...
Delete
Items per page : 50 Page : -
Restore files to
Original location
Alternate location : C:\Alternate Location
Change
Search
Previous
Start Restore
Cancel

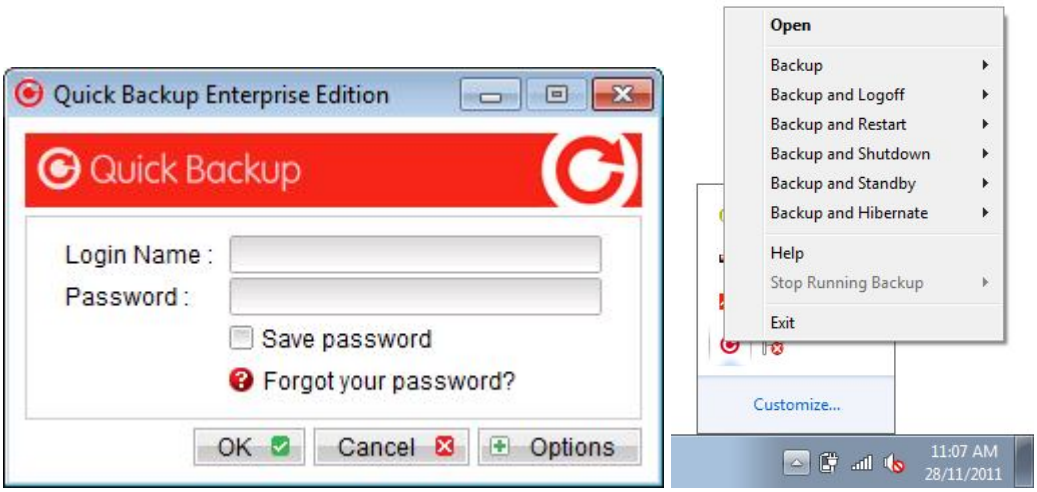
4. Click the [Start Restore] button to begin the restore process.

5. When the restore process is completed, the virtual machines will be restored to the original hypervisor.

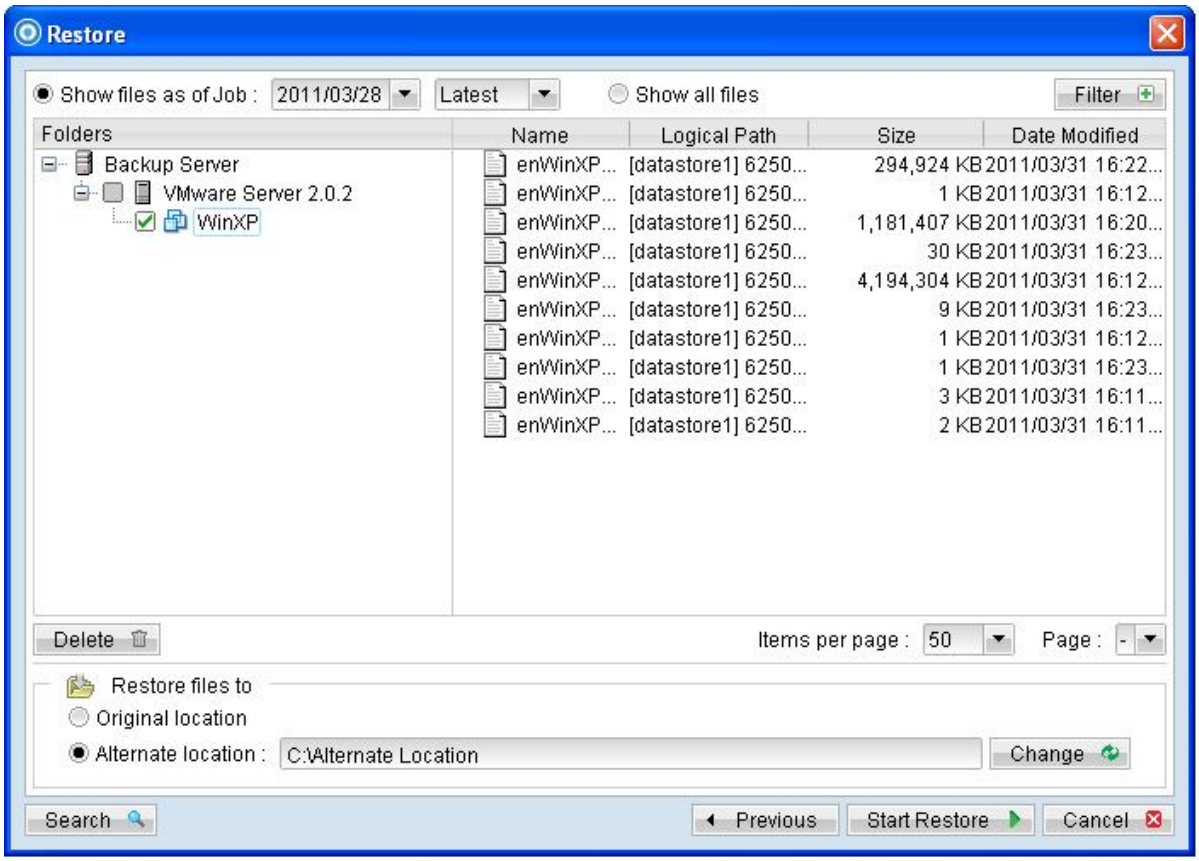
Restoring to another hypervisor:

1. Login to the backup application's user interface.

2.

3. 

4. Select the [Restore] button and the corresponding backup set.



5. Select the virtual machines to be restored and choose [Alternate location] for restore files to.

6. Click on the [Change] button and browse to the directory path which you would like to restore the data to.

7. Click the [Start Restore] button to begin the restore process.

8. When the restore process is completed, data of the selected virtual machines will be restored to the specified location.

9. Re-register the virtual machines on the new hypervisor.

   Please consult your VMware hypervisor administrator for more details.

13.3 Independent disk for VMware virtual machine

Online backup cannot be performed on virtual machines with Independent Disk (snapshot cannot be created for Independent Disk), Quick Backup will skip the backup of all Independent Disk(s) during backup.

When these VMs are restored to original hypervisor, Independent Disks that were not backed up will be missing, Quick Backup would modify the *.VMX file according to the missing disk to allow the machine to be powered on.

Note:
Quick Backup will backup the original *.vmx file with a suffix .orig.

However, the machine may not work properly due to the missing disk.

14 Backup / Restore Microsoft Virtual Machines

This chapter describes how to backup and restore virtual machines running on Microsoft Windows Hyper-V Server (Non-Cluster or Cluster environment).

14.1 Backup virtual machines running on Hyper-V Server (Non-Cluster environment)

14.1.1 Requirements and Recommendations

Please ensure that the following requirements are met by the backup client computer:

1. Quick Backup version 6.7 or above is installed on the Hyper-V server
2. The Hyper-V management tools are installed on the Hyper-V server.
3. Consider increasing the JVM (Java Virtual Machine) memory allocation to improve performance of the backup operation.
4. It is recommended that the temporary directory have disk space of at least 50% of the largest sized virtual machine to be backed up.
5. It is recommended that the temporary directory be configured on a local drive.

14.1.2 Limitations

The following are limitations of the MS VM backup module:

1. **Important:** Virtual machines backed up with the MS VM backup module **can only** be restored to the original Hyper-V server.
2. Backup of virtual machine with pass through disk (directly attached physical disk) is not supported.

14.1.3 Overview

The following steps take place when a virtual machine backup is performed with Quick Backup:

1. Connection from the backup client to the backup server is established.
2. Download the server file list from the backup server.
3. Commands are issued to the hypervisor to create snapshot (e.g. memory dump) of the virtual machine with Volume Shadow Copy.

Important:

- The corresponding virtual machine will be paused during the snapshot process, it will automatically resume when the operation is completed.

- Do not attempt to start the virtual machine while it is in the saving state. The snapshot created may be invalid and the backup may not be usable for restore operations

- The corresponding virtual machine uptime (in Hyper-V Manager) will be reset to 00:00:00.

4. After generating all files, the files are copied to the temporary directory and upload to Quick Backup Server.

5. Commands are issued to the hypervisor to remove the Volume Shadow Copy snapshot created.

6. Backup completed successfully.

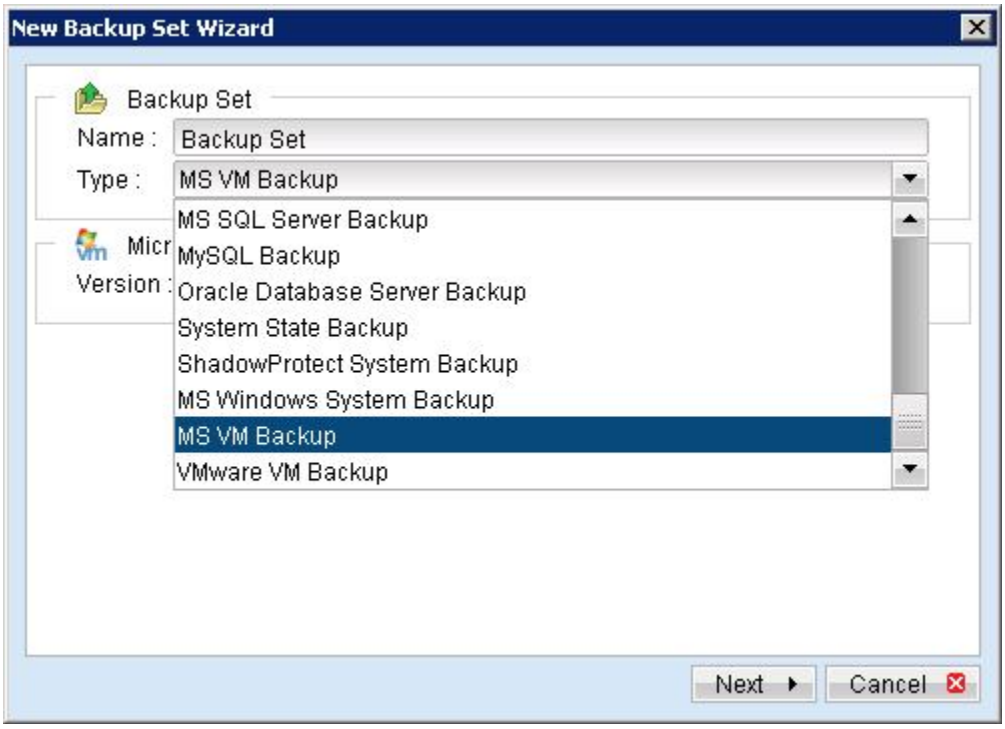
14.1.4 How to Backup Microsoft Virtual Machines

Refer to the follow instructions to backup virtual machines running on Microsoft Hyper-V Server:

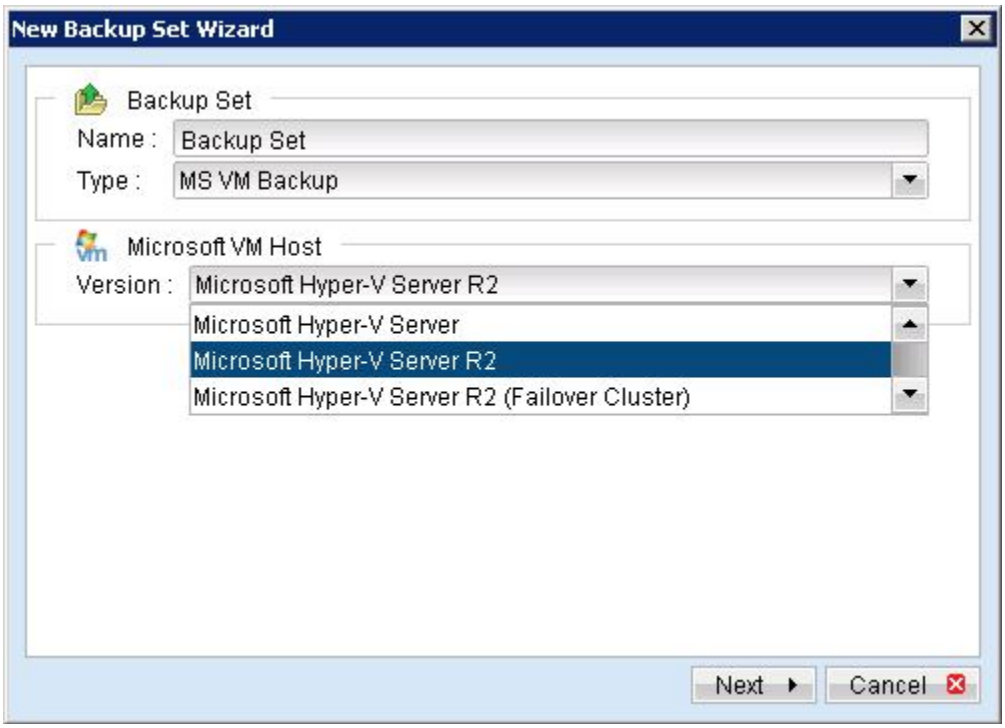
1. Login to the backup application's user interface.

2. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

3. Create a MS VM Backup set by selecting [MS VM Backup] from the backup set type dropdown menu.

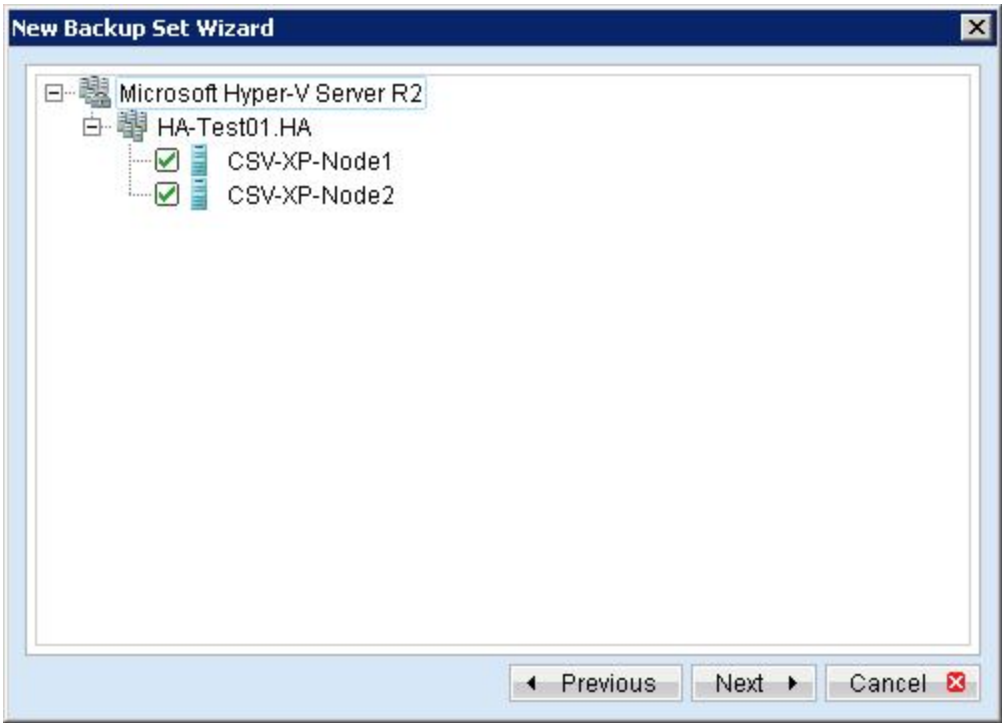


4. Select the version of the hypervisor.



5. Select [Next] to proceed.

6. Select the corresponding virtual machines for backup.



7. Configure a backup schedule for unattended backups.

8. Select an encryption setting for your backup set.

9. Press the [OK] button to complete the configuration of backup set.

10. Scheduled backup will run automatically if you leave your computer on.
11. To perform a backup immediately, click [Backup] button on the left panel.

14.1.5 How to Restore Microsoft Virtual Machines

Refer to the follow instructions to restore virtual machines running on Hyper-V.

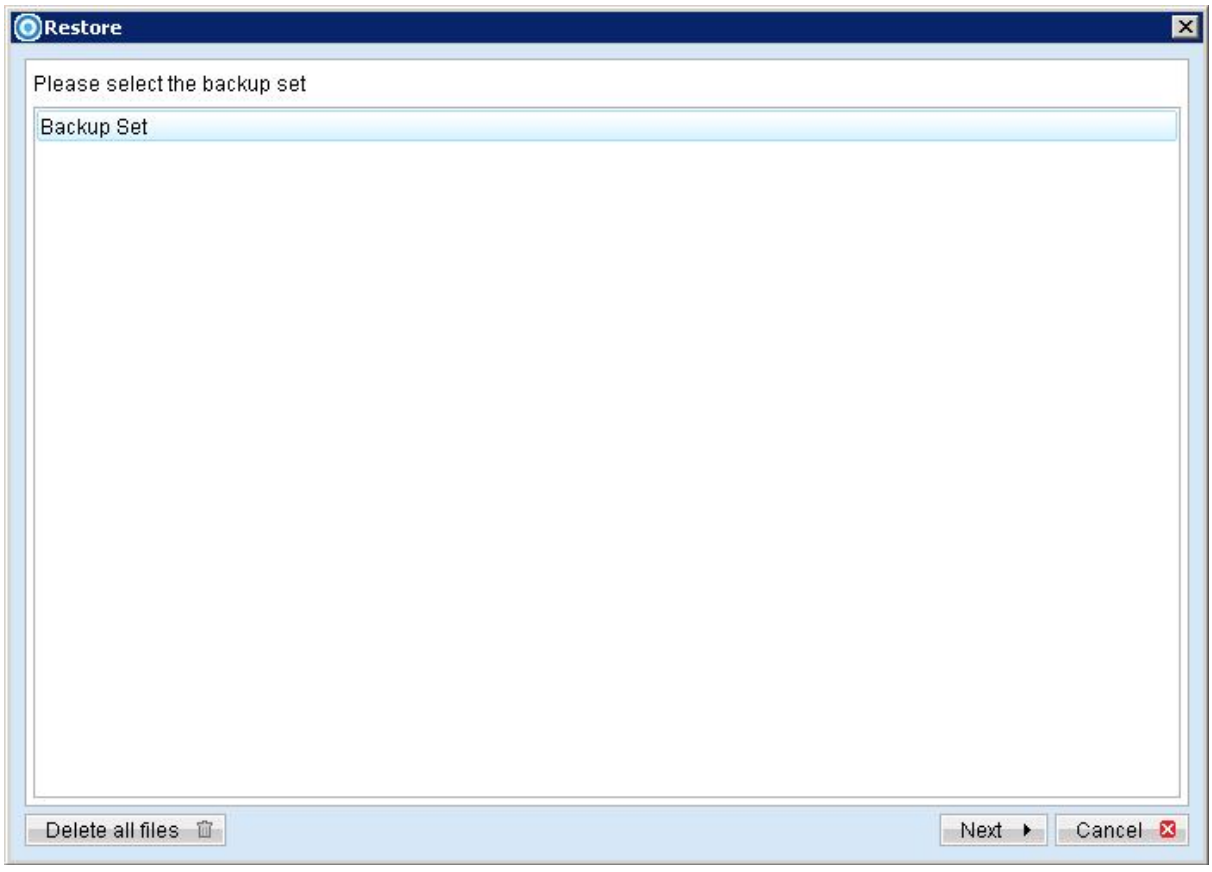
The virtual machine will be restored under the following conditions:

- If the virtual machine to be restored no longer exist on the original hypervisor. The VM will be restored as a new virtual machine.
- If the virtual machine to be restored still exist on the original hypervisor. The existing VM will be replaced by the backed up version.

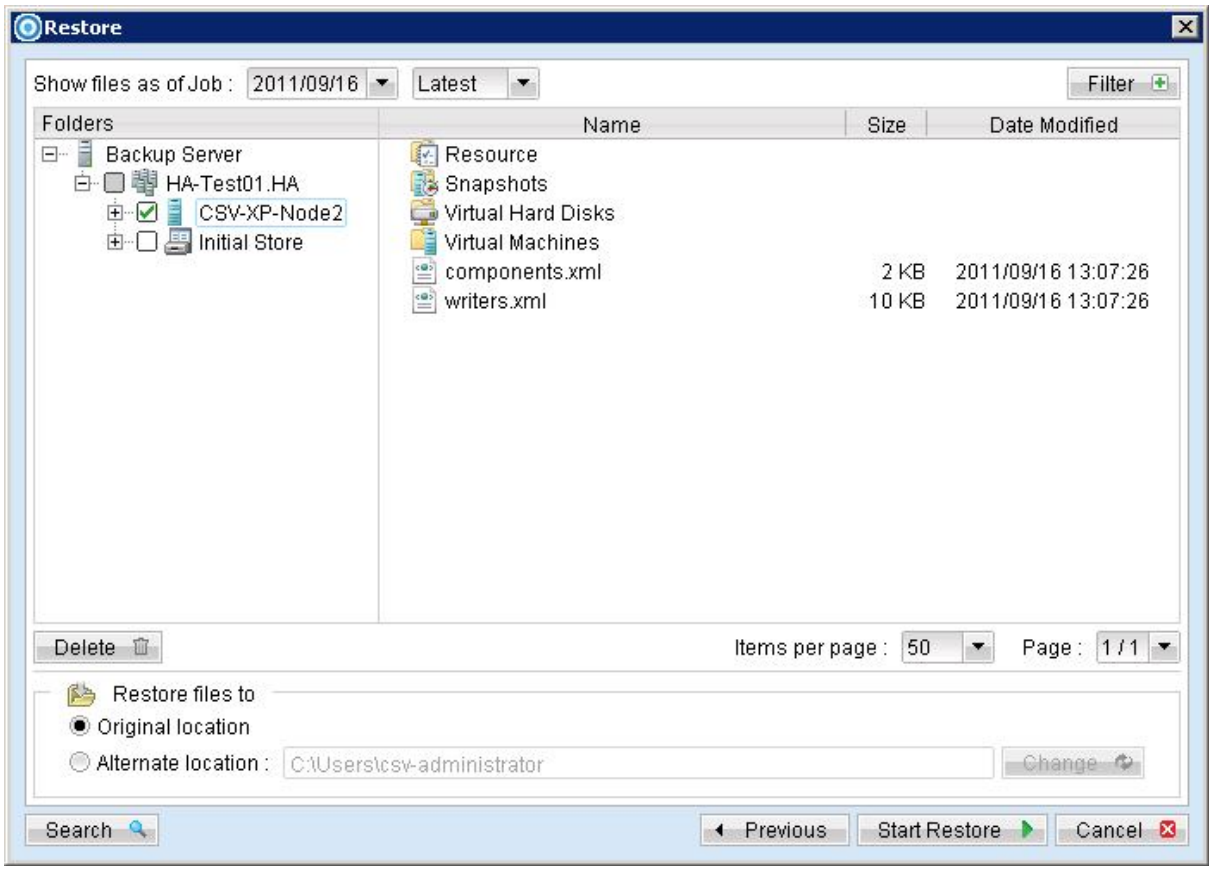
Important:
Virtual machines backed up with the MS VM backup module **can only** be restored to the original Hyper-V server.

1. Login to the backup application's user interface.

2. Select the [Restore] button and the corresponding backup set.



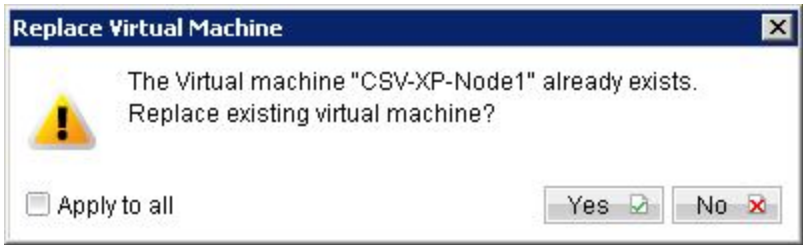
3. Select the virtual machines to be restored and choose [Original Location] for restore files to.



Note:
Select the Initial Store if you want to restore the Authorization Manager Security (role-based access control) settings

4. Click the [Start Restore] button to begin the restore process.

5. User will be prompted if a virtual machine selected to be restored exist on the hypervisor.



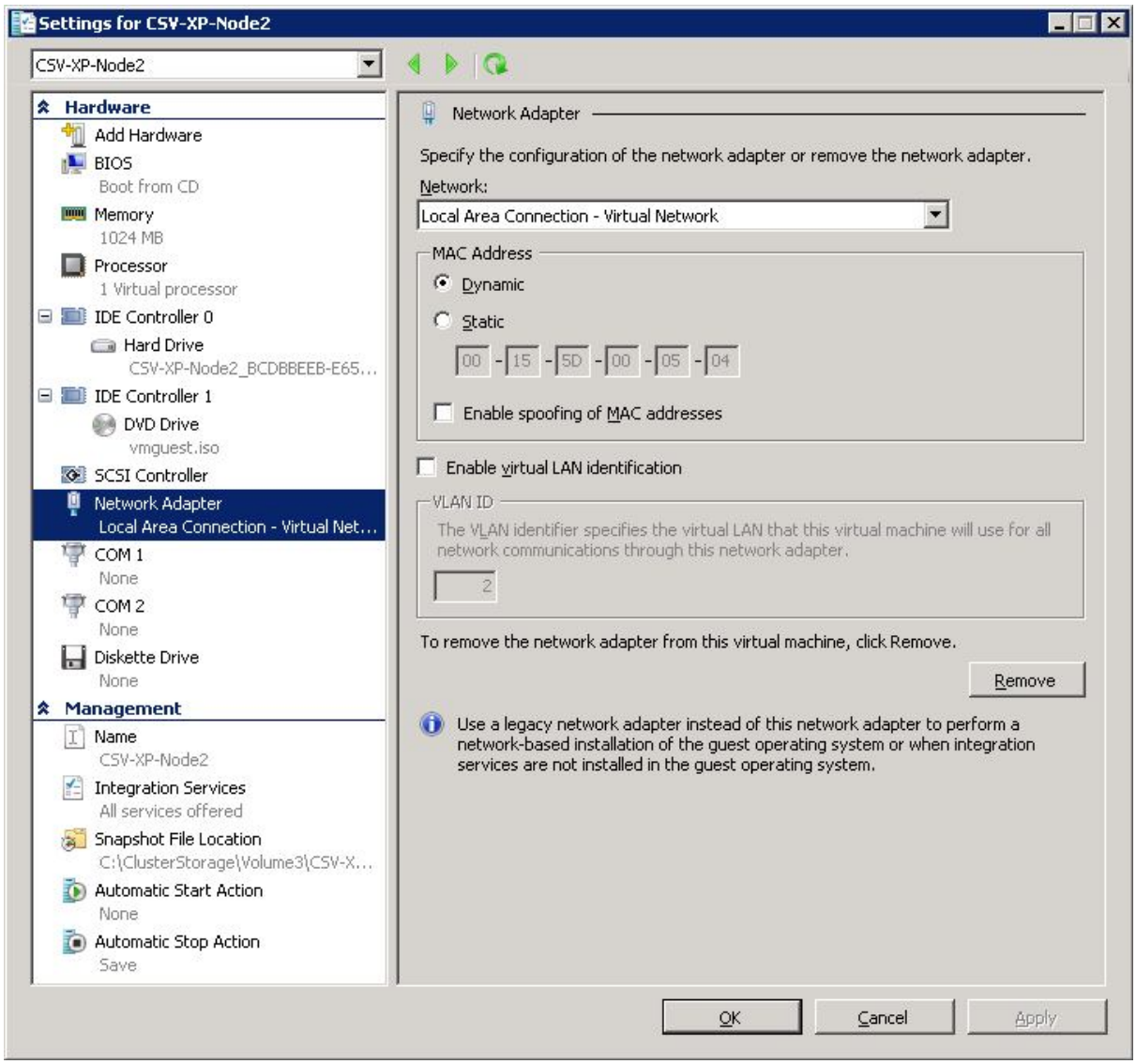
Important:
For restore of **existing virtual machine** (restoring a previous version), the existing virtual machine will be removed before the restore process begin.

6. When the restore process is completed, the virtual machines will be restored to the original hypervisor.

7. Open Hyper-V Manager, click Start, Administrative Tools and click Hyper-V Manager.

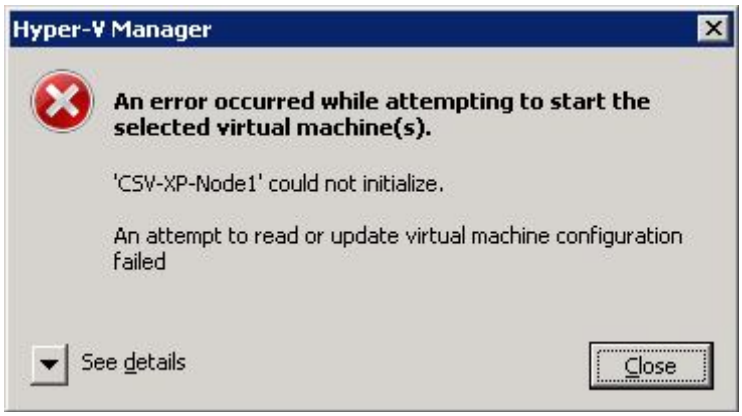
8. Under Virtual Machines, right-click on the newly restored virtual machine, select Setting.

9. Modify settings which may be conflicting with other existing virtual machines (e.g. network setting).



10. Start the virtual machine.

Note:
The following error may be displayed when starting the VM.


Hyper-V Manager
An error occurred while attempting to start the selected virtual machine(s).
'CSV-XP-Node1' could not initialize.
An attempt to read or update virtual machine configuration failed
See details
Close

Please remove the Saved State of the corresponding VM. Under Virtual Machines, right-click on the VM and select **Delete Saved State...**, start the VM again afterward.

11. The restore process is now completed.

14.2 Backup virtual machines running on Hyper-V Server (Cluster environment)

14.2.1 Requirements and Recommendations

Please ensure that the following requirements are met by the backup client computer:

1. Quick Backup version 6.7 or above is installed on all Hyper-V cluster nodes.
2. The Hyper-V management tools are installed on all Hyper-V cluster nodes.
3. Consider increasing the JVM (Java Virtual Machine) memory allocation to improve performance of the backup operation.
4. It is recommended that the temporary directory have disk space of at least 50% of the largest sized virtual machine to be backed up.
5. It is recommended that the temporary directory be configured on a local drive.

14.2.2 Limitations

The following are limitations of the MS VM backup module:

1. **Important:** Virtual machines backed up with the MS VM backup module **can only** be restored to the original Hyper-V server.
2. Backup of virtual machine with pass through disk (directly attached physical disk) is not supported

14.2.3 Overview

The following steps take place when a virtual machine backup is performed with Quick Backup:

3. Connection from the backup client to the backup server is established.

4. Download the server file list from the backup server.

5. Commands are issued to the hypervisor to create snapshot (e.g. memory dump) of the virtual machine with Volume Shadow Copy.

   Important:
   - The corresponding virtual machine will be paused during the snapshot process, it will automatically resume when the operation is completed.

   - The corresponding virtual machine uptime (in Hyper-V Manager) will be reset to 00:00:00.

6. After generating all files, the files are copied to the temporary directory and upload to Quick Backup Server.

7. Commands are issued to the hypervisor to remove the Volume Shadow Copy snapshot created.

8. Backup completed successfully.

14.2.4 How to Backup Microsoft Virtual Machines in Cluster Environment

Refer to the follow instructions to backup virtual machines running on Microsoft Hyper-V Server in Cluster environment:

1. Install Quick Backup on all Hyper-V cluster nodes.

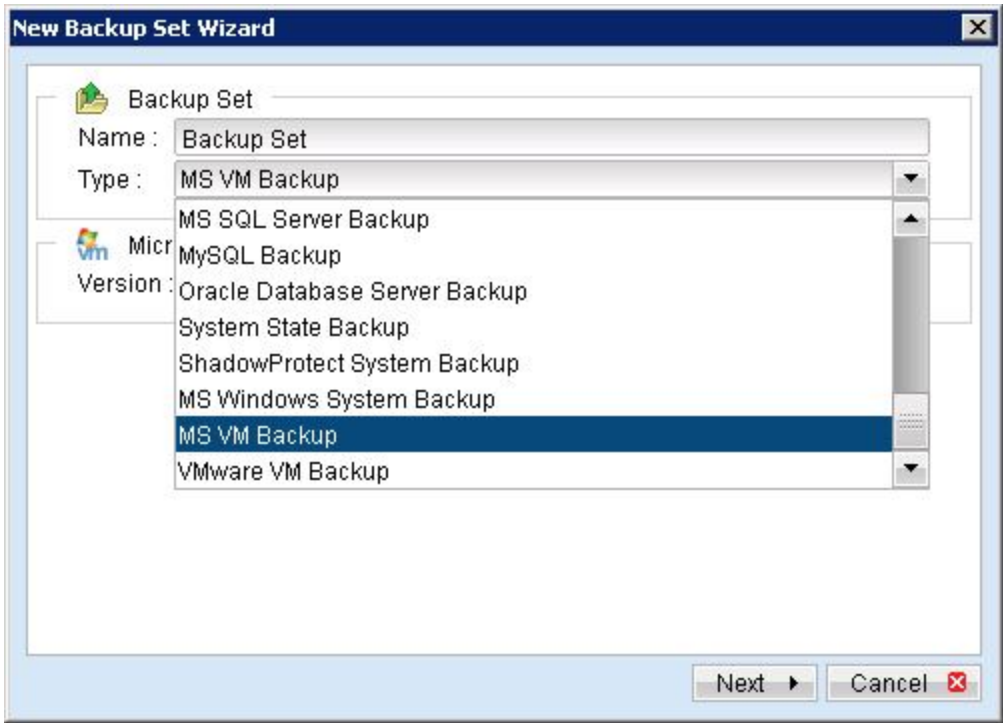
2. On each cluster node, login to the backup application's user interface.

3. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

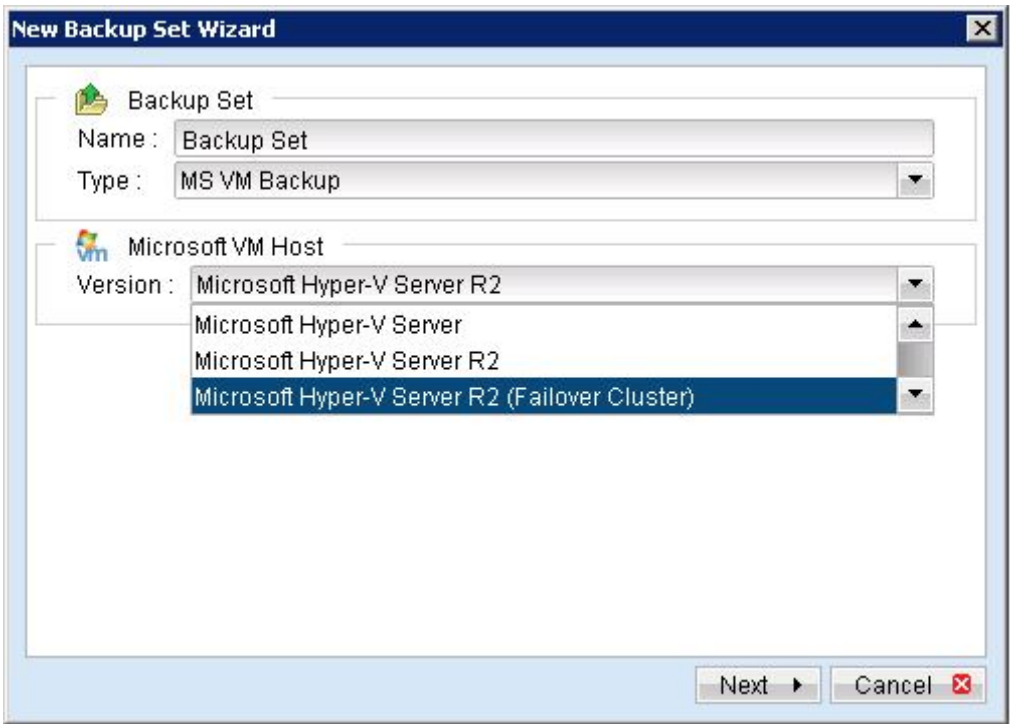
4. Create a separate MS VM Backup set for each cluster node.

   Important:
   Each cluster node **must** have its own unique MS VM backup set.

5. On each node, select [MS VM Backup] from the backup set type dropdown menu.



6. Select [Microsoft Hyper-V Server R2 (Failover Cluster)].

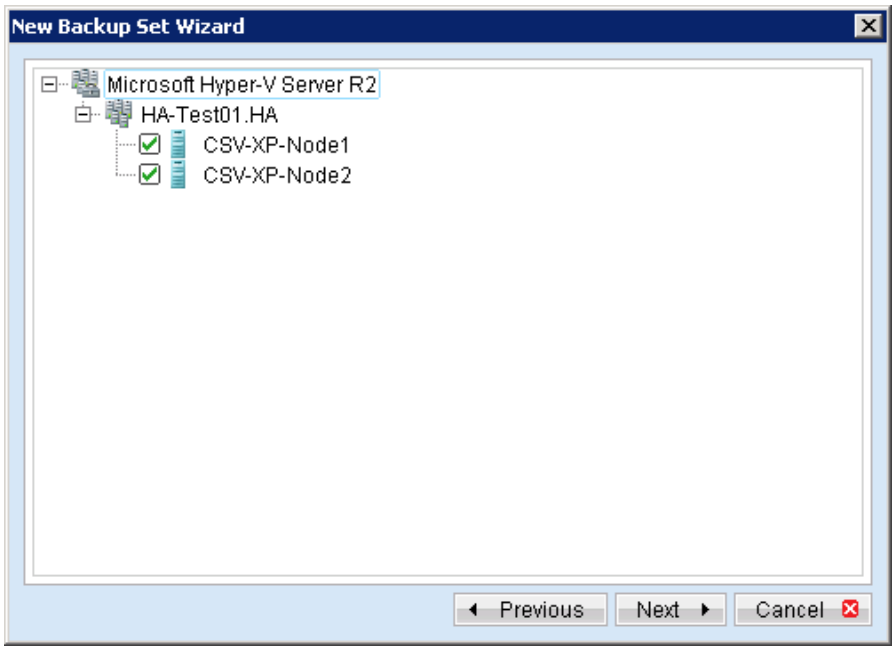


7. Select [Next] to proceed.

8. In the backup source selection screen, select the virtual machines for backup.

   Note:
   Virtual machines of all cluster nodes will be shown in the backup selection screen.

9. To backup all VMs within the cluster setup, select all VMs listed.



   Note:
   Even with all VMs selected, only VMs that are own by the current node will be backed up (for each respective backup set). Other VMs will be skipped automatically.

10. Configure a backup schedule for unattended backups.
11. Select an encryption setting for your backup set.
12. Press the [OK] button to complete the configuration of backup set.
13. Scheduled backup will run automatically if you leave your computer on.
14. To perform a backup immediately, click [Backup] button on the left panel.

14.2.5 How to Restore Microsoft Virtual Machines in Cluster Environment

Refer to the follow instructions to restore virtual machines running on Hyper-V in cluster environment.

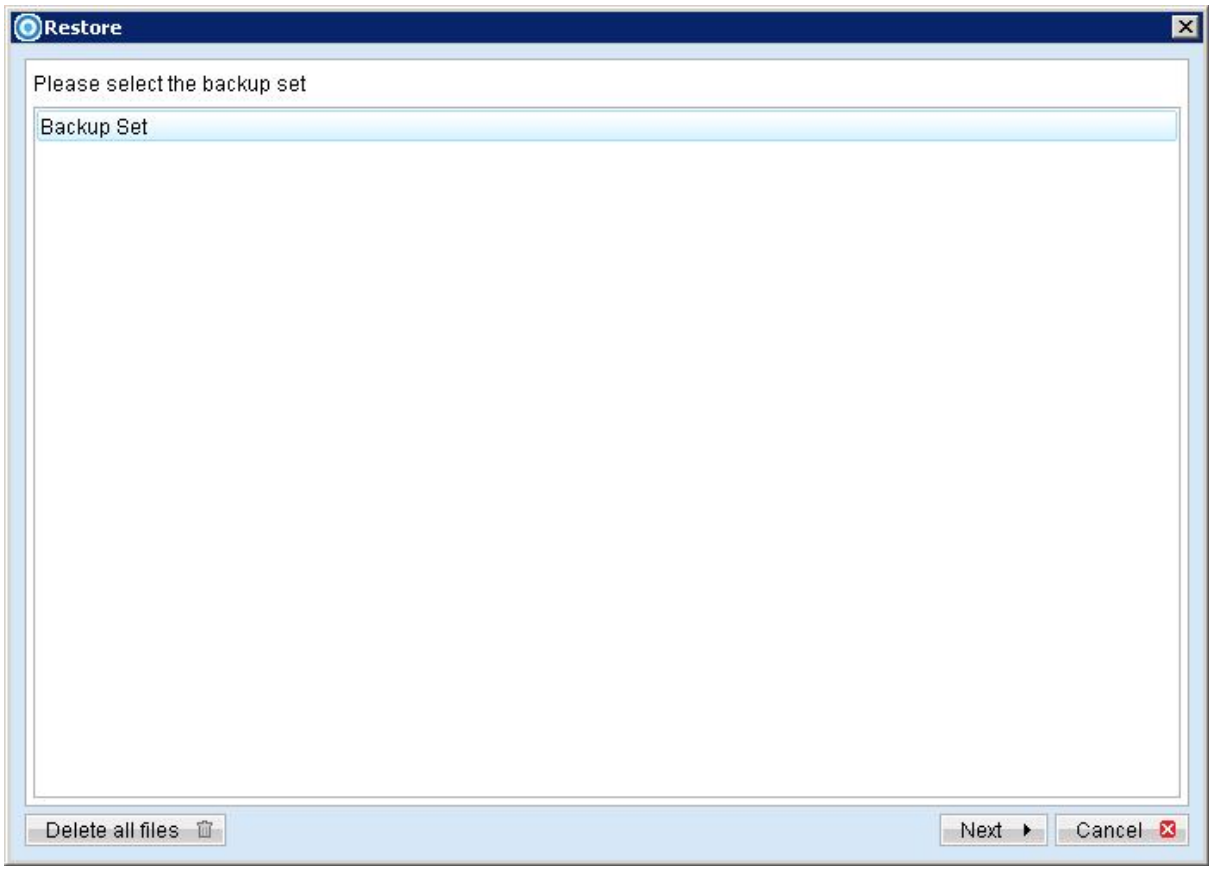
The virtual machine will be restored under the following conditions:

- If the virtual machine to be restored no longer exist on the original hypervisor. The VM will be restored as a new virtual machine.
- If the virtual machine to be restored still exist on the original hypervisor. The existing VM will be replaced by the backed up version.

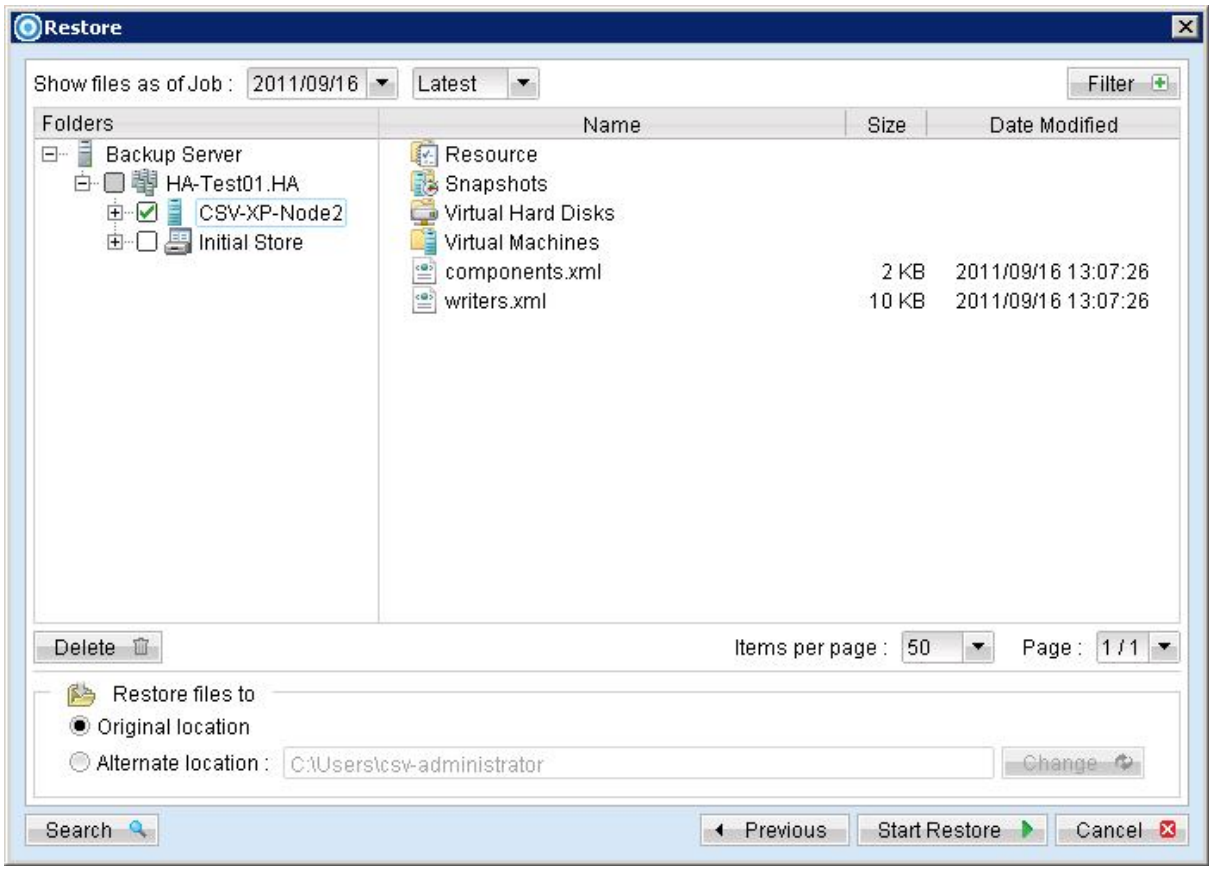
Important:
Virtual machines backed up with the MS VM backup module **can only** be restored to the **original Hyper-V cluster node**.

1. On the original Hyper-V cluster node, login to the backup application's user interface.

2. Select the [Restore] button and the corresponding backup set.



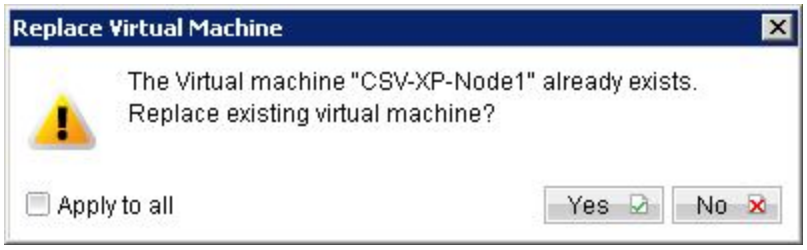
3. Select the virtual machines to be restored and choose [Original Location] for restore files to.



Note:
Select the Initial Store if you want to restore the Authorization Manager Security (role-based access control) settings.

4. Click the [Start Restore] button to begin the restore process.

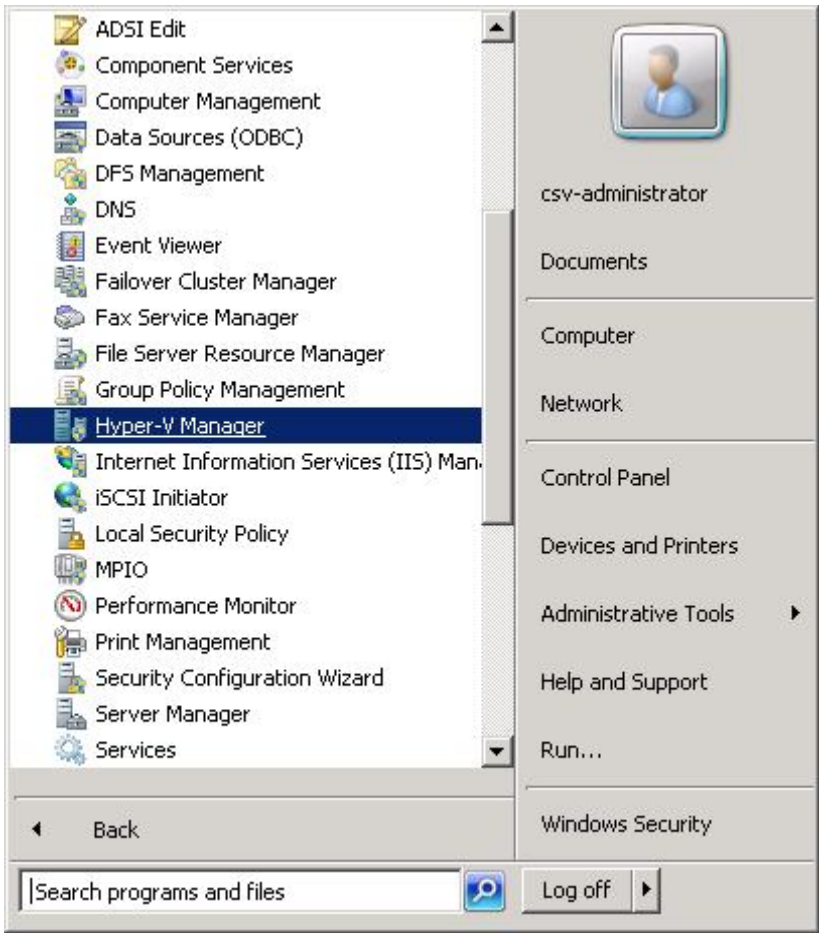
5. User will be prompted if a virtual machine selected to be restored exist on the hypervisor



Important:
For restore of **existing virtual machine** (restoring a previous version), the existing virtual machine will be removed before the restore process begin.

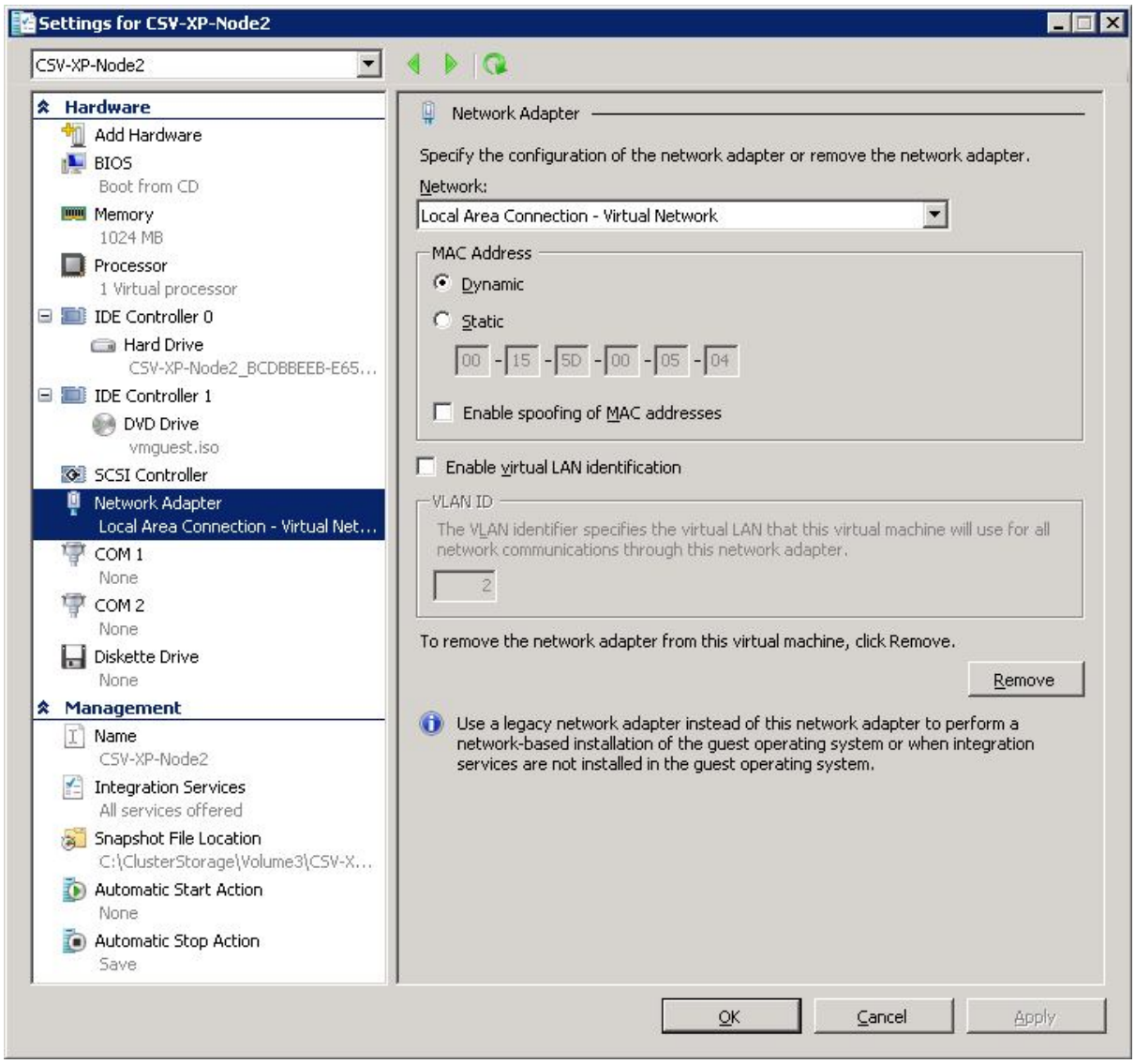
6. When the restore process is completed, the virtual machines will be restored to the original hypervisor.

7. Open Hyper-V Manager, click Start, Administrative Tools and click Hyper-V Manager.



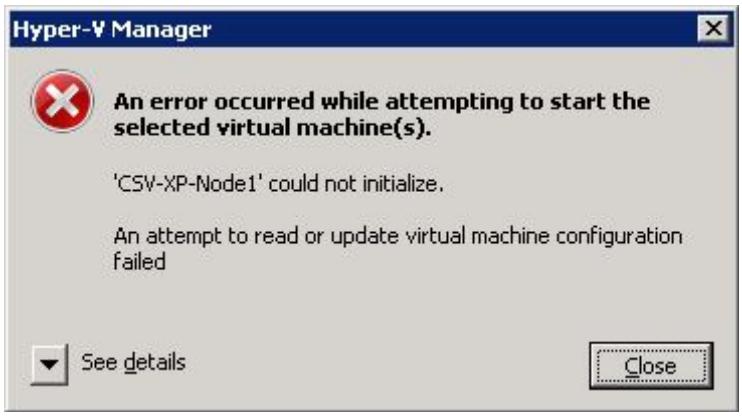
8. Under Virtual Machines, right-click on the newly restored virtual machine, select Setting.

9. Modify settings which may be conflicting with other existing virtual machines (e.g. network setting).



10. Start the virtual machine.

    Note:
    The following error may be displayed when starting the VM.


Hyper-V Manager
An error occurred while attempting to start the selected virtual machine(s).
'CSV-XP-Node1' could not initialize.
An attempt to read or update virtual machine configuration failed
See details
Close

    Please remove the Saved State of the corresponding VM. Under Virtual Machines, right-click on the VM and select **Delete Saved State...**, start the VM again afterward.

11. The restore process is now completed.

15 Backup / Restore Microsoft Exchange Server

This chapter describes how to backup and restore Microsoft Exchange Server.

15.1 Supported versions

The MS Exchange Server backup module is supported for the following Exchange versions:

- MS Exchange 2003
- MS Exchange 2007
- MS Exchange 2010

15.2 Backup Microsoft Exchange Server 2003 / 2007

15.2.1 Requirements and recommendations

Please ensure that the following requirements are met by the MS Exchange server:

1. Quick Backup is installed on the Exchange server.

2. Databases of the Exchange server are spooled to a temporary directory before being uploaded to the offsite backup server.

   It is recommended that the temporary directory have disk space of at least 120% of the total database size (e.g. total size of all .edb files found within the MS Exchange Server installation folder).

3. It is recommended that the temporary directory be configured on a local drive.

15.2.2 Overview

For a complete Exchange server backup, backup for the following components must be performed:

Windows System State
With every Exchange server backup, it is recommended to perform a System State backup, which secures the system state data.

As part of Exchange Database restores in the future, the system state must be restored as well. Running regular system state backups of the Exchange is therefore crucial, as it ensures that the system state data is synchronized with the Exchange database data, so that it can be properly restored if the need arises.

Microsoft Information Store (Exchange 2003 / 2007)
The Information Store of Exchange 2003 or 2007 contains both mailbox store and public folder store data. The server stores data in two files: an .edb file and a .stm file.

Together, the .edb file and the .stm file form an Exchange store repository. For example, the default mailbox store on an Exchange server uses files named Priv1.edb and Priv1.stm. The default public folder store uses the files Pub1.edb and Pub1.stm.

The .edb file contains many tables that hold metadata for all e-mail messages and other items in the Exchange store, in addition to the contents of MAPI messages. The .stm file, in contrast, stores native Internet content.

15.2.3 How to backup Microsoft Exchange Server 2003 / 2007

Refer to the follow instructions to backup Microsoft Exchange Server 2003 / 2007:

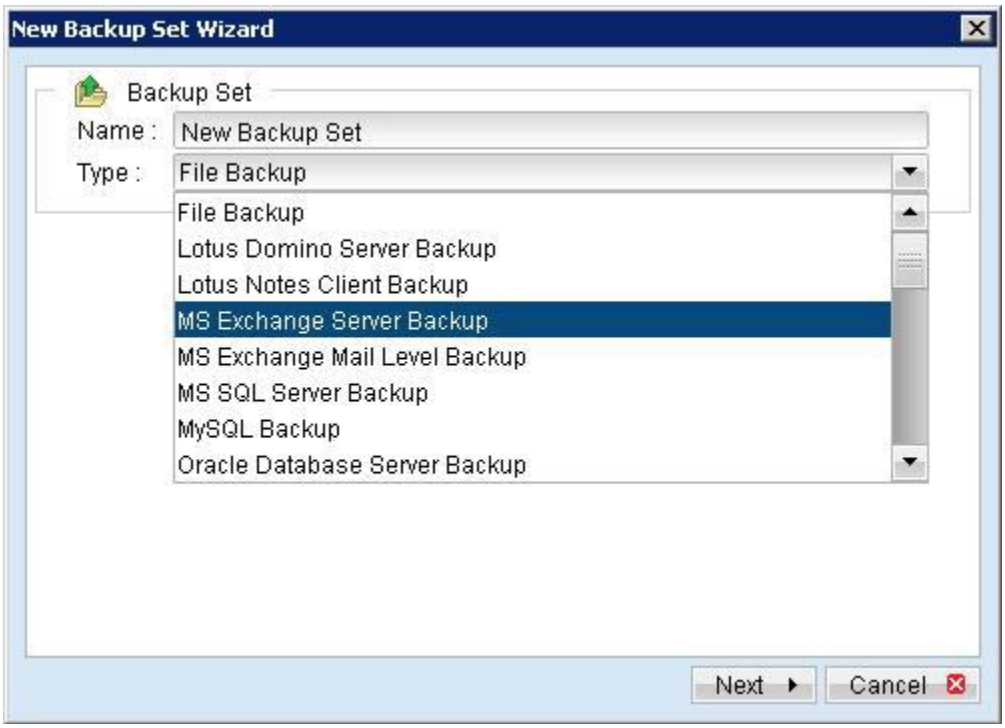
1. Open Quick Backup. Right click Quick Backup icon available in the system tray and choose [Open].

2. Create a backup set.

   i. To start setting up backup sets, click the button to open the [Backup Setting] dialog.

   ii. On the left panel, press the button to create a new backup set.

   iii. On the dialog, choose [MS Exchange Server Backup] as the [Type].



iv. Enter a name for your backup set.

v. Choose the correct Exchange Server version from the [Version] drop down box.

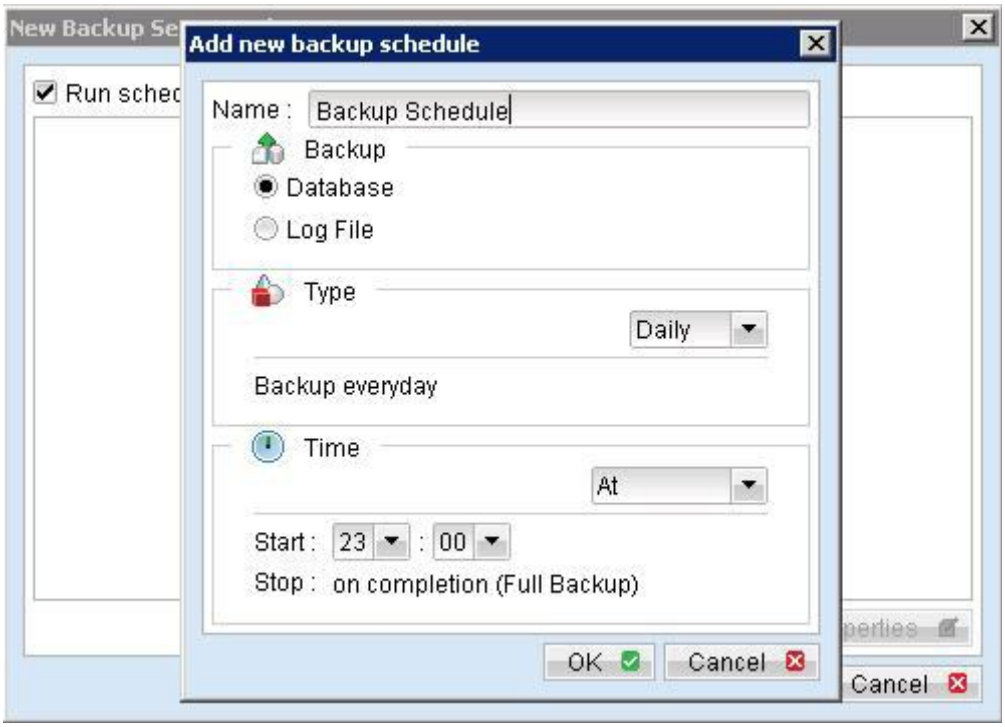
vi. Select the database(s) to be backed up.

If this Exchange Server is also a domain controller of this Active Directory, select the [System State] checkbox as well. Otherwise, please install Quick

Backup to the domain controller of this Active Directory and select the [System State] checkbox on that computer.

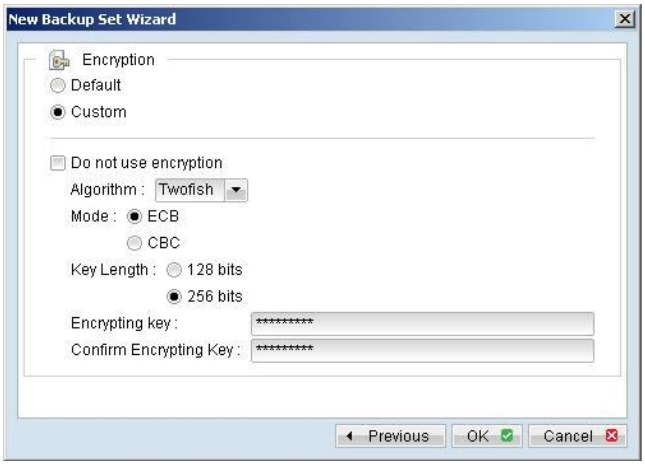
vii. Enter a temporary directory for storing the backup files before they are sent to Quick Backup Server.

viii. Set the backup schedule for Database Backup.



ix. Set the backup schedule for Transaction Log Backup.

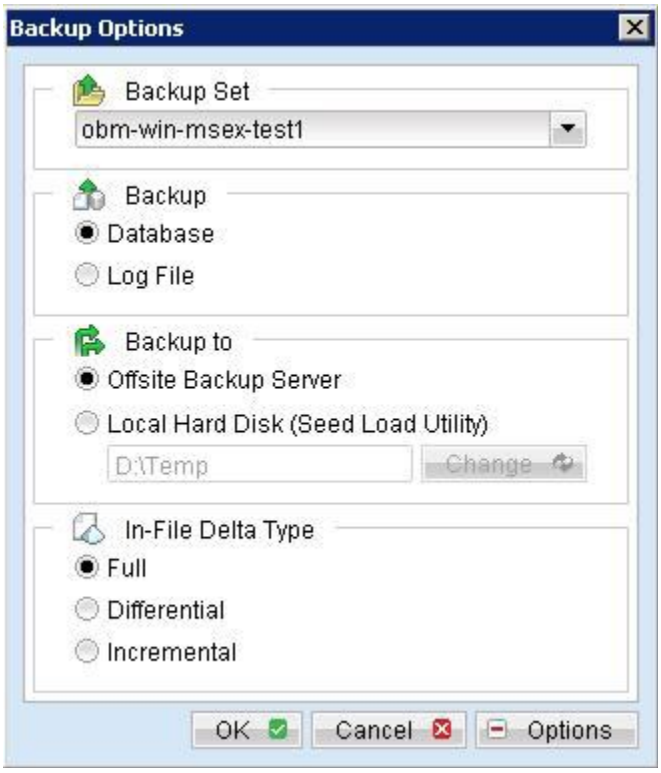
x. Set the encryption algorithm, encryption mode and encrypting key for this backup set.



3. Performing backup.

i. Press the [Backup] button on the main page of Quick Backup dialog.

ii. Select the backup type (e.g. Database, Log Files) you would like to perform. Select the backup set you want to run and select [Offsite Backup Server] to start backing up your files to Quick Backup Server. If applicable, you can change the In-File Delta Type also.

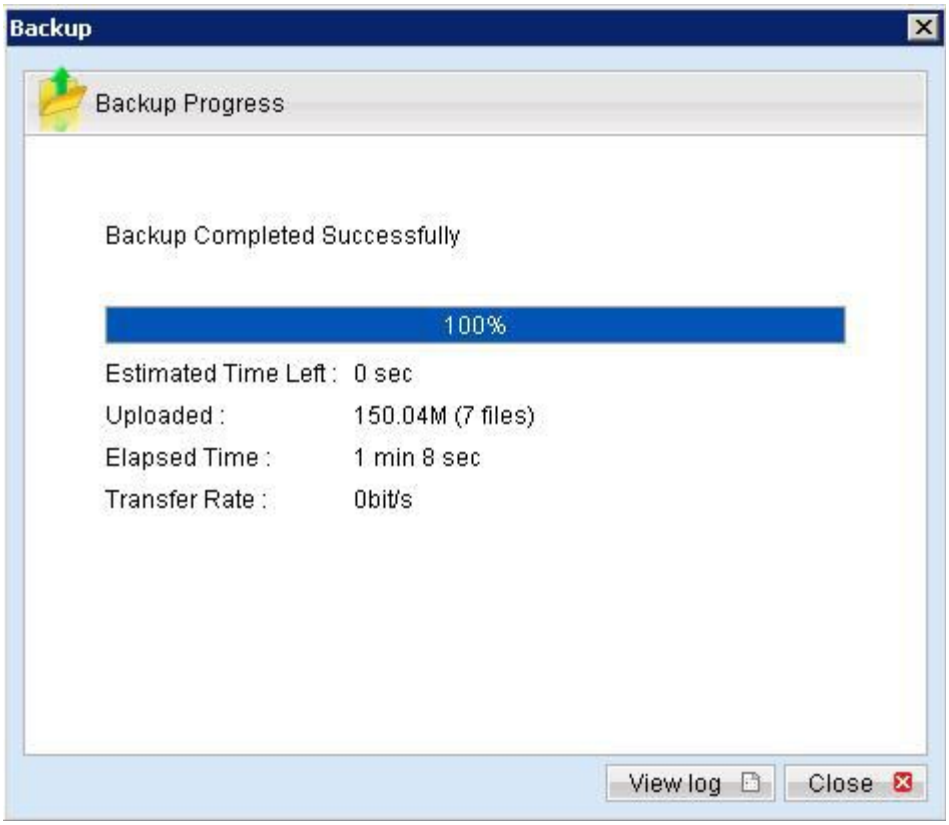


Backup Type:

Backup Type	Descriptions
Full	Backup the databases and transaction logs and then truncates the transaction logs.
Incremental	Backup the transaction logs to record changes since the last full or incremental backup and then truncates the transaction logs.
Differential	Backup the transaction logs to record changes since the last full or incremental backup and does not truncate the transaction logs.

iii. Click [OK] to start backing up your files to Quick Backup Server.

iv. You should get something similar to the screen shot below:



Note:
If your Exchange Server is also a domain controller, please go to the Windows System State Section to setup a Windows System State Backup.

15.3 Restore Microsoft Exchange Server 2003 / 2007

Please follow the instructions below to restore Microsoft Exchange Server from Quick Backup Server:

1. Prepare the system for your Exchange Server (if required).

   Install the original version of Windows and Exchange Server (with the same level of service pack installed as in the original system) back to your computer.

2. Restore Windows Active Directory (if required).

   If you have re-installed Windows, please download the Windows System State backup file, named [SystemState.bkf], from Quick Backup Server and then use [NTBackup.exe] to restore your Windows System State to its backup time from the backup file by following the instructions below:

   i. Run [NTBackup.exe] from [Start] > [Run].

   ii. Press the [Next] button to go to [Backup or Restore Wizard].

   iii. Select the [Restore files and settings] checkbox and press the [Next] button.

   iv. Double click an item on the left and select the checkbox of any drive/folder/file that you want to restore.

   v. Press the [Next] button and then the [Finish] button.

3. Install Quick Backup (if required).

   Please refer to the Installation section for information on how to install Quick Backup onto your computer.

4. Startup the [Microsoft Information Store] services from Windows Services.

5. Restore exchange database(s) from backup:

   i. Download the database backup files to be restored from the Quick Backup Server (or find the cached copy available in the temporary directory defined in your backup set) and save them to your hard disk (Please make sure the directory structure is the same as it appears on the browser):

```
->[C:]
-->[backup]
---->[SERVER]
------>[Microsoft Information Store]
-------->[First Storage Group]
---------->[Mailbox Store(SERVER)]
---------------->Priv1.edb
---------------->Priv1.stm
---------->[Public Folder Store(SERVER)]
---------------->Pub1.edb
---------------->Pub1.stm
```

```
---------->E0000001.log
```

ii. If the database to be restored exists on your computer already, please dismount it from the services using [Start] > [Program] > [Microsoft Exchange] > [System Manager].

iii. Use [ExchangeRestore.exe] from the [bin] directory under the installation directory of Quick Backup (e.g. C:\Program Files\Quick Backup\bin\ExchangeRestore.exe) to restore the exchange database(s).

iv. (Example 1) To restore all databases from backup available in [F:\Backup] to an Exchange Server named “WIN2000SVR" using the temporary directory F:\temp, you can use this command:

```
E:\Program Files\Quick Backup\bin> ExchangeRestore DIR="f:\Backup"
TEMP="f:\Temp" SERVER="WIN2000SVR"
```

Exchange Server Recovery Example

```
E:\Program Files\Quick Backup\bin> ExchangeRestore DIR="F:\Backup"
TEMP="F:\Temp" SERVER="WIN2000SVR"

Microsoft Exchange Server 2000/2003 Backup Recovery Utility

 [Start] Exchange Server - 'WIN2000SVR'
  [Start] Service - 'Microsoft Information Store'
   [Start] Storage Group - 'First Storage Group'
    [Start] Database - 'Mailbox Store (WIN2000SVR)'
     Restoring file 'E:\Program Files\Exchsrvr\mdbdata\priv1.edb' ...
     Restoring file 'E:\Program Files\Exchsrvr\mdbdata\priv1.stm' ...
    [End] Database - 'Mailbox Store (WIN2000SVR)'
    [Start] Database - 'Public Folder Store (WIN2000SVR)'
     Restoring file 'E:\Program Files\Exchsrvr\mdbdata\pub1.edb' ...
     Restoring file 'E:\Program Files\Exchsrvr\mdbdata\pub1.stm' ...
    [End] Database - 'Public Folder Store (WIN2000SVR)'
    [Start] Restoring transaction log - 'First Storage Group'
     Restoring Log File 'F:\Temp\restore.tmp\First Storage
Group\E00000B3.log' ...
     Restoring Log File 'F:\Temp\restore.tmp\First Storage
Group\E00000B4.log' ...
    [End] Restoring transaction log - 'First Storage Group'
    [Start] Applying transaction log ...
    [End] Applying transaction log
   [End] Storage Group - 'First Storage Group'
…
   [Start] Storage Group - 'SG2'
    [Start] Database - 'acct'
     Restoring file 'E:\Program Files\Exchsrvr\SG2\acct.edb' ...
     Restoring file 'E:\Program Files\Exchsrvr\SG2\acct.stm' ...
    [End] Database - 'acct'
```

```
    [Start] Restoring transaction log - 'SG2'
     Restoring Log File 'F:\Temp\restore.tmp\SG2\E0100072.log' ...
     Restoring Log File 'F:\Temp\restore.tmp\SG2\E0100073.log' ...
    [End] Restoring transaction log - 'SG2'
    [Start] Applying transaction log ...
    [End] Applying transaction log
   [End] Storage Group - 'SG2'
[End] Exchange Server - 'WIN2000SVR'

E:\Program Files\Quick Backup\bin>
```

v. (Example 2) To restore the database named “mail" in storage group “SG5" from backup available in f:\Backup to an exchange server named “WIN2000SVR" using the temporary directory “F:\temp" , you can use this command:

E:\Program Files\Quick Backup\bin> ExchangeRestore DIR="f:\Backup" TEMP="f:\Temp" SERVER="WIN2000SVR" SERVICE="Microsoft Information Store" STORAGE="SG5" DATABASE="mail1"

Exchange Server Recovery Example:

```
E:\Program Files\Quick Backup\bin> ExchangeRestore DIR="F:\Backup"
TEMP="F:\Temp" SERVER="WIN2000SVR" SERVICE="Microsoft Information
Store" STORAGE="SG5" DATABASE="mail"

Microsoft Exchange Server 2000/2003 Backup Recovery Utility

   [Start] Storage Group - 'SG5'
    [Start] Database - 'mail'
     Restoring file 'E:\Program Files\Exchsrvr\SG5\mail.edb' ...
     Restoring file 'E:\Program Files\Exchsrvr\SG5\mail.stm' ...
    [End] Database - 'mail'
    [Start] Restoring transaction log - 'SG5'
     Restoring Log File 'F:\Temp\restore.tmp\SG5\E0300012.log' ...
     Restoring Log File 'F:\Temp\restore.tmp\SG5\E0300013.log' ...
    [End] Restoring transaction log - 'SG5'
    [Start] Applying transaction log ...
    [End] Applying transaction log
   [End] Storage Group - 'SG5'

E:\Program Files\Quick Backup\bin>
```

vi. Repeat the same procedure for each database to be restored to the Exchange Server.

vii. You can use [Start] > [Program] > [Administrative Tools] > [Event Viewer] to check if there are errors generated from the Exchange databases restoring activities.

6. However, if ExchangeRestore.exe still cannot mount the restored files and returns with strange errors, e.g. bad signature, or null errors, the Exchange server might have incorrectly spooled the backup files in the first place.

   Please try to mount the restored database and log files manually by the following instructions:

   i. In MS Exchange System Manager, dismount both the Mailbox Store and Public Folder Store from the server.

   ii. Copy all the restored database files to the MDBDATA folder (BY default, the MDBDATA folder is located under C:\Program Files\Excgsrvr\).

   iii. Run “eseutil /r" to apply the transaction log files to bring the database to a consistent state, e.g.:

   ```
   C:\Program Files\Exchsrvr\MDBDATA> ..\bin\eseutil /r e00
   ```

   iv. Run “eseutil /p" to repair the database files, e.g.:

   ```
   C:\Program Files\Exchsrvr\MDBDATA> ..\bin\eseutil /p priv1.edb

   C:\Program Files\Exchsrvr\MBDATA> ..\bin\eseutil /p pub1.edb
   ```

   v. Mount both Mailbox Store and Public Folder Store to the Server through the MS Exchange System Manager.

7. The restore of Exchange Server is now completed.

15.4 Backup Microsoft Exchange Server 2010

15.4.1 Requirements and recommendations

Please ensure that the following requirements are met by the MS Exchange server:

1. Quick Backup version 5.5.8.0 or above is installed on the Exchange server.

2. Databases of the Exchange server are spooled to a temporary directory before being uploaded to the offsite backup server.

   It is recommended that the temporary directory have disk space of at least 120% of the total database size (e.g. total size of all .edb files found within the MS Exchange Server installation folder).

3. It is recommended that the temporary directory be configured on a local drive.

4. Backup of Exchange 2010 server in Database Availability Group (DAG) is currently not supported.

15.4.2 Overview

For a complete Exchange server backup, backup for the following components must be performed:

Windows System State
With every Exchange server backup, it is recommended to perform a System State backup, which secures the system state data.

As part of Exchange Database restores in the future, the system state must be restored as well. Running regular system state backups of the Exchange is therefore crucial, as it ensures that the system state data is synchronized with the Exchange database data, so that it can be properly restored if the need arises.

Microsoft Information Store (Exchange 2010)
The Information Store of Exchange 2010 contains the data, data definitions, indexes, checksums, flags, and other information that comprise mailboxes in Exchange. Mailbox databases hold data that's private to an individual user and contain mailbox folders generated when a mailbox is created for that user. A mailbox database is stored as an Exchange database .edb file.

Public folder databases contain the data, data definitions, indexes, checksums, flags, and other information that comprise any public folders in your Exchange organization

15.4.3 How to backup Microsoft Exchange Server 2010

Refer to follow the instructions to backup Microsoft Exchange Server 2010:

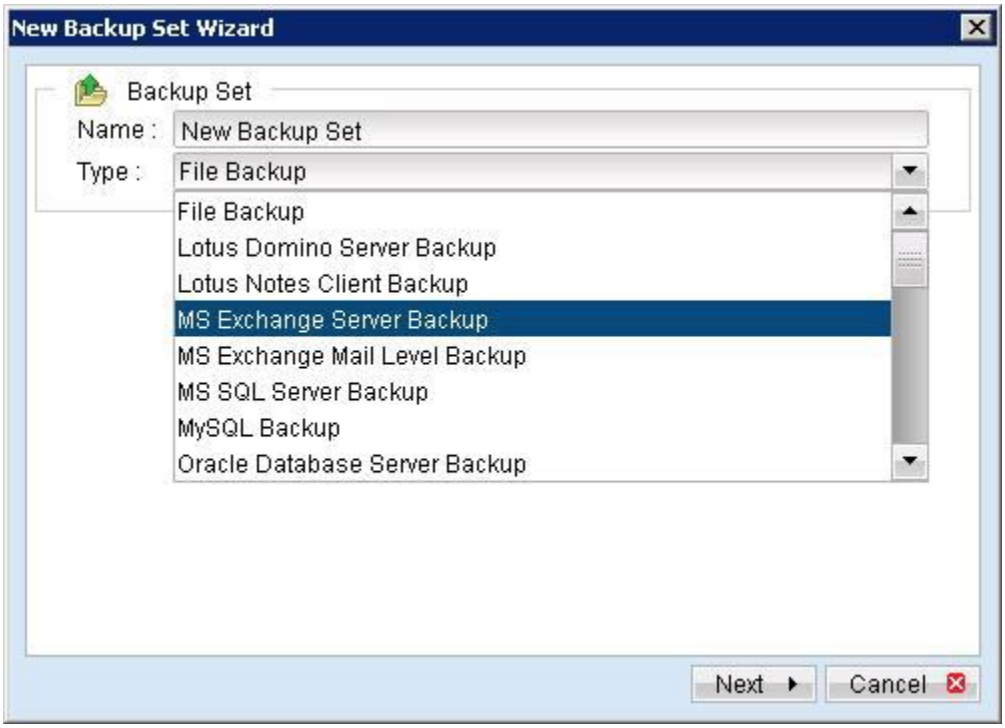
1. Open Quick Backup. Right click Quick Backup icon available in the system tray and choose [Open].

2. Create Backup set.

i. To start setting up backup sets, click the button to open the [Backup Setting] dialog.

ii. On the left panel, press the button to create a new backup set.

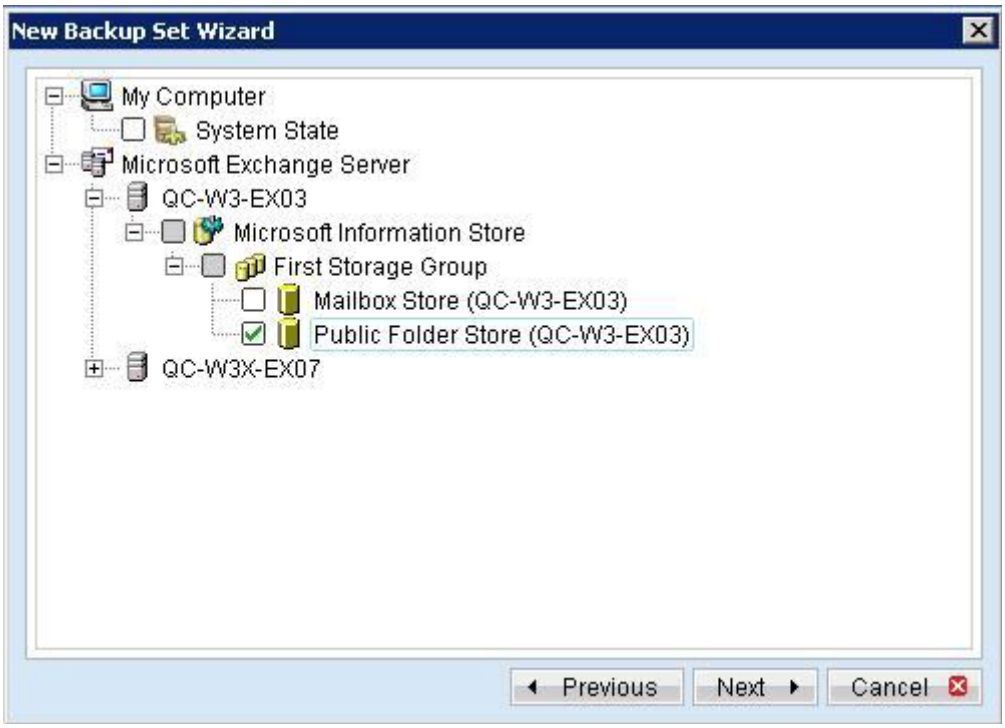
iii. On the dialog, choose [MS Exchange Server Backup] as the [Type].



iv. Enter a name for your backup set.

v. Choose the correct Exchange Server version from the [Version] drop down box.

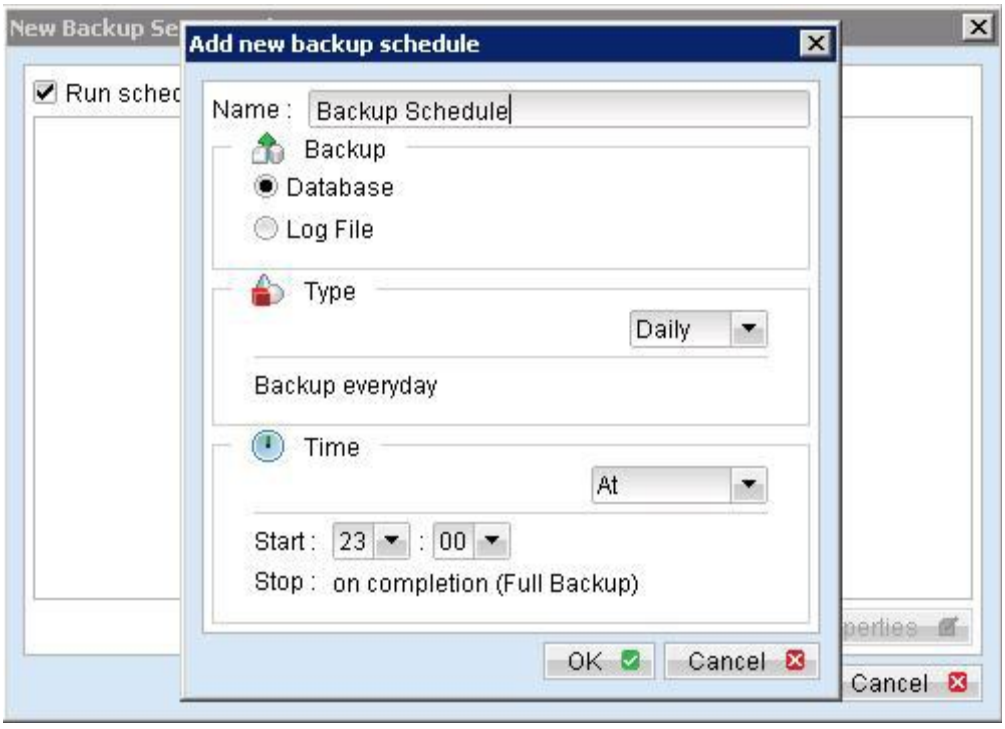
vi. Select the database(s) to be backed up.



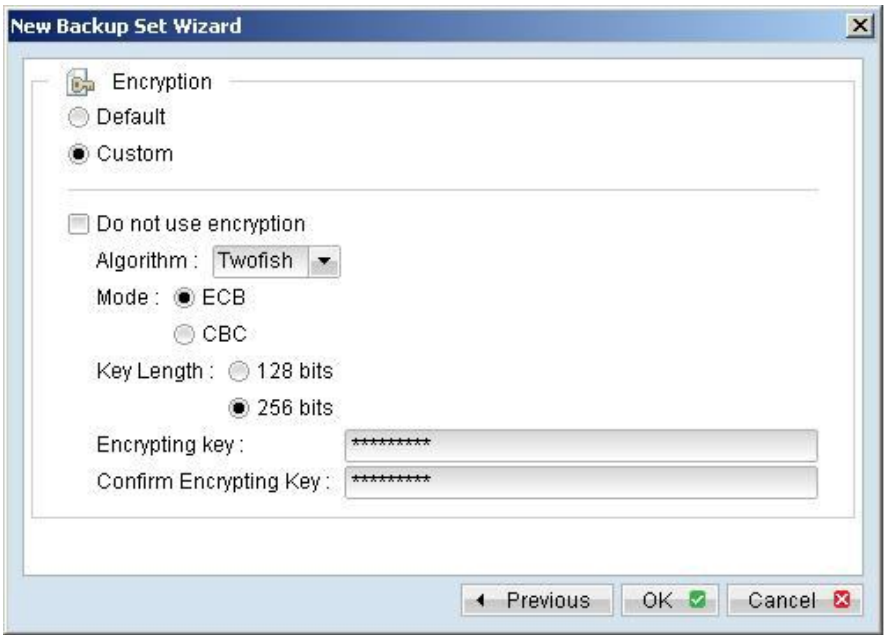
If this Exchange Server is also a domain controller of this Active Directory, select the [System State] checkbox as well. Otherwise, please install Quick Backup TO THE DOMAIN CONTROLLER OF HTSI Active Directory and select the [System State] checkbox on that computer.

vii. Enter a temporary directory for storing the backup files before they are sent to Quick Backup Server.

viii. Set the backup schedule for Database Backup.



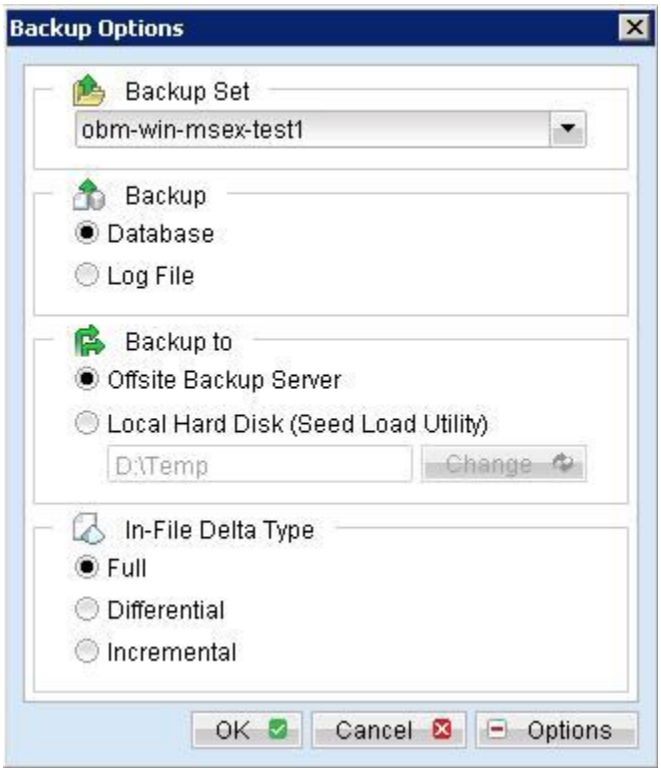
ix. Set the encryption algorithm, encryption mode and encrypting key for this backup set.



3. Run Backup.

i. Press the [Backup] button on the main page of Quick Backup dialog.

ii. Select the backup type (e.g. Database, Log Files) you would like to perform. Select the backup set you want to run and select [Offsite Backup Server] to start backing up your files to Quick Backup Server. If applicable, you can change the In-File Delta Type also.

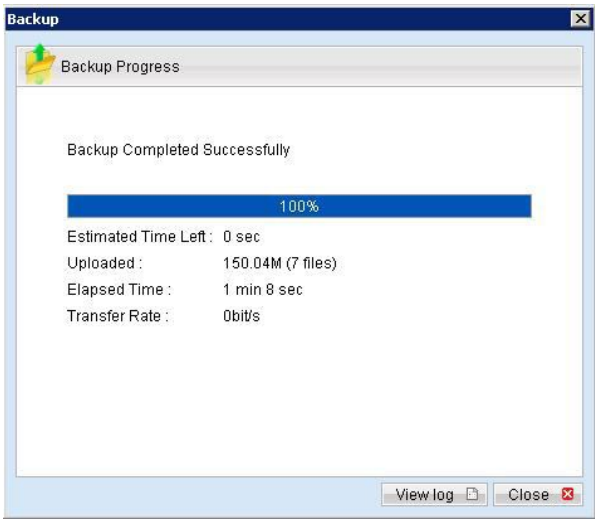


Backup Type:

Backup Type	Descriptions
Full	Backup the databases, transaction logs, checkpoint files and then truncates the transaction logs.
Copy	Backup the databases, transaction logs, checkpoint files but does not truncate the transaction logs.
Incremental	Backup the transaction logs to record changes since the last full or incremental backup and then truncates the transaction logs.
Differential	Backup the transaction logs to record changes since the last full or incremental backup and does not truncate the transaction logs.

iii. Click [OK] to start backing up your files to Quick Backup Server.

iv. You should get something similar to the screen shot below:



Note:
If your Exchange Server is also a domain controller, please go the Windows System State section to setup a Windows System State Backup.

15.5 Restore Microsoft Exchange Server 2010

Please follow the instructions below to restore Microsoft Exchange Server 2010 from Quick Backup Server.

1. Prepare the system for your Exchange Server (if required).

   Install the original version of Windows and Exchange Server 2010 (with the same level of service pack installed as in the original system) back to your computer.

2. Restore Windows Active Directory (if required).

   If you have re-installed Windows, please restore the Windows System State from a Windows System State Backup set.

3. Install Quick Backup (if required).

   Please refer to the installation section for the instruction on how to install Quick Backup onto your computer.

4. Startup the [Microsoft Information Store] services from Windows Services.

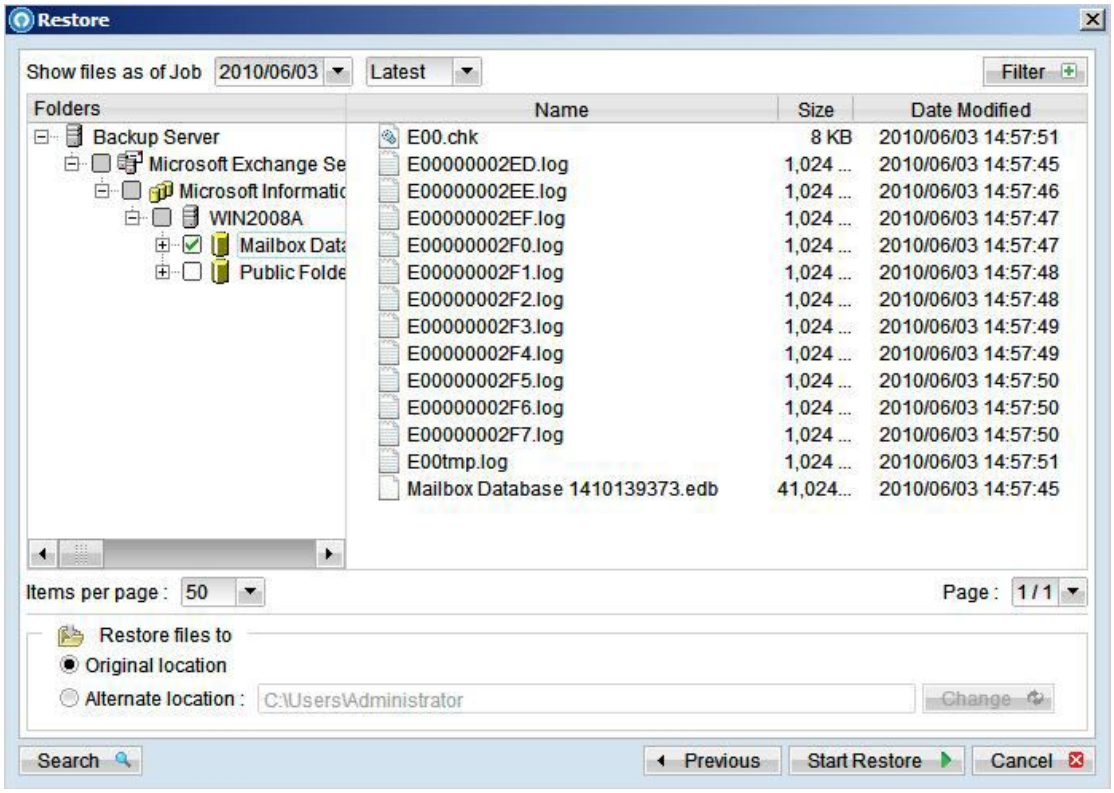
5. Restore Windows System State. Please refer to Windows System State Section for more information.

6. Restore Exchange database(s) from backup.

Restore Exchange Database(s) to Original Location

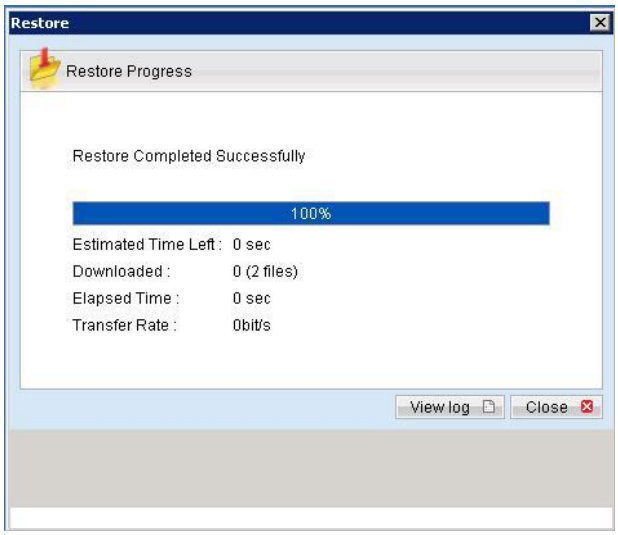
To restore Exchange Server 2010 to the same location, please follow the steps below:

1. Select the database to be restored and choose [Original Location], all necessary files would download automatically.



2. Press the [Start Restore] button to restore.

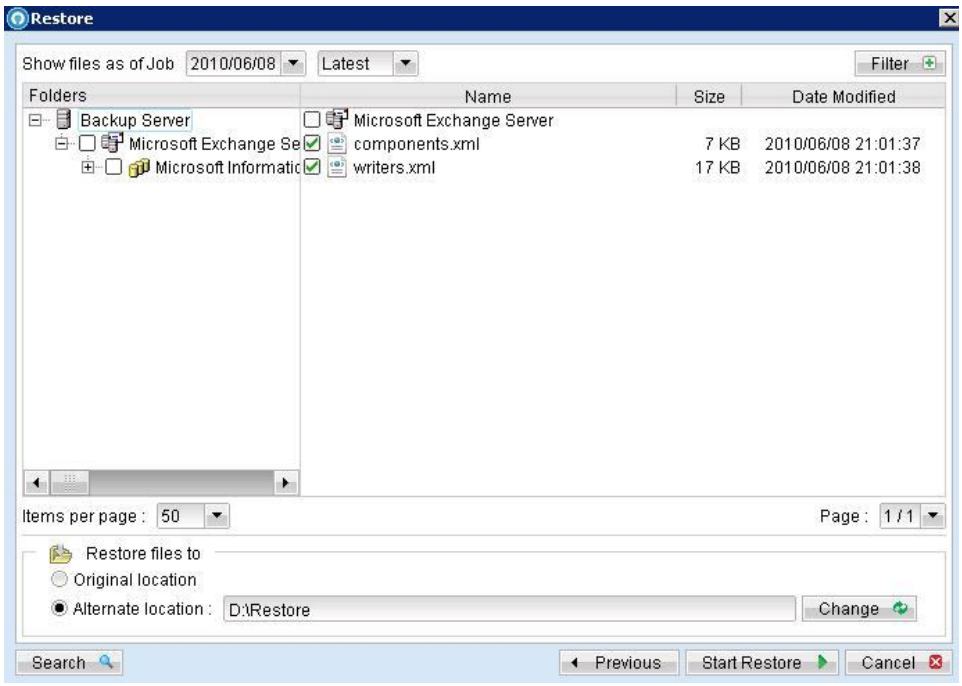
3. The restore process is now completed.



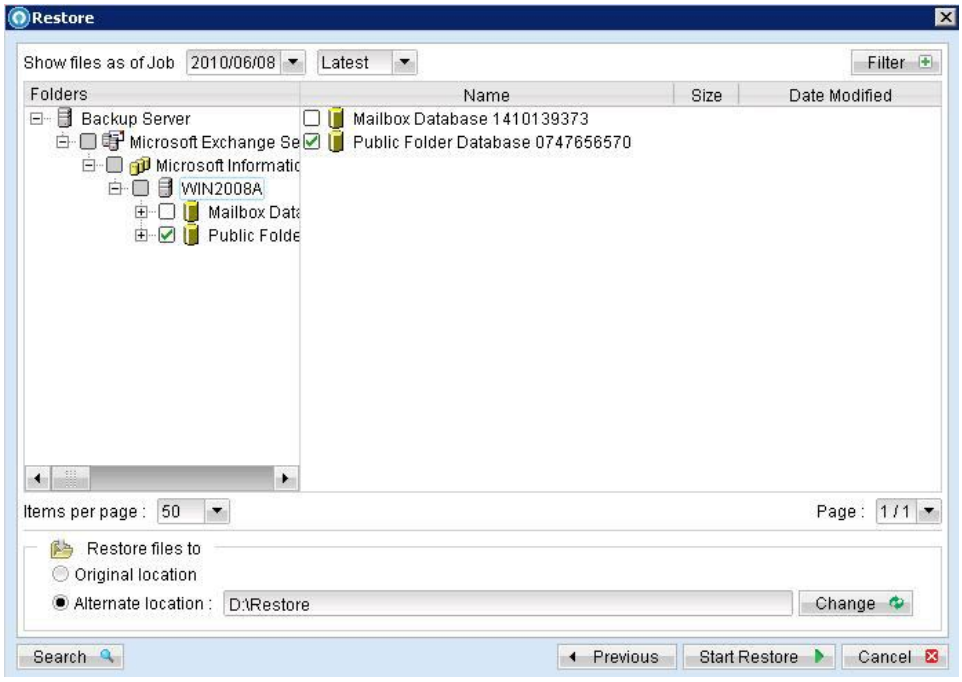
Restore Exchange Database(s) to Alternate Location

To restore Exchange Server 2010 to an alternate location, please follow the steps below:

1. Download the database backup files to be restored from the Quick Backup Server (or find the cached copy available in the temporary directory defined in your backup set). First, choose components.xml and writer.xml from the file list.



2. Then select the database that you are going to restore.



3. Restore the database(s) to your hard disk. Please make sure the directory structure is the same as it appears on the browser:

```
->[D:]
-->[Restore]
---->[Microsoft Exchange Server] [components.xml][writers.xml]
```

```
------>[Microsoft Information Store]
-------->[SERVER_NAME]
--------->[DATABASE_NAME]
```

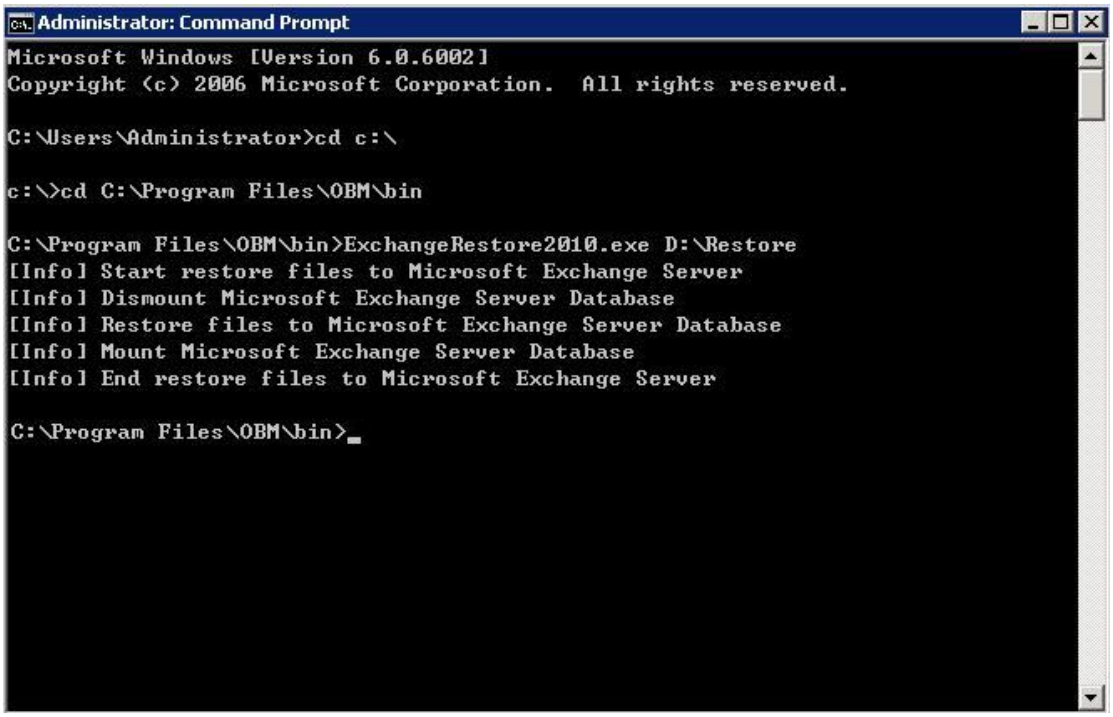
4. Use [ExchangeRestore2010.exe] from *%Quick Backup_HOME%\bin* to restore the exchange database(s).

5. To restore databases from backup available in *D:\Restore*, you can use this command.

C:\Program Files\OBM\bin> ExchangeRestore2010 D:\Restore:

Or

C:\Program Files\Quick Backup\bin> ExchangeRestore2010 D:\Restore:


Administrator: Command Prompt
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>cd c:\
c:\>cd C:\Program Files\OBM\bin
C:\Program Files\OBM\bin>ExchangeRestore2010.exe D:\Restore
[Info] Start restore files to Microsoft Exchange Server
[Info] Dismount Microsoft Exchange Server Database
[Info] Restore files to Microsoft Exchange Server Database
[Info] Mount Microsoft Exchange Server Database
[Info] End restore files to Microsoft Exchange Server
C:\Program Files\OBM\bin>

6. The restore process is now completed successfully.

16 Brick-Level Backup/Restore Microsoft Exchange Server

This chapter describes in details how to use the Exchange Brick-Level Backup features in Quick Backup to backup individual items (e.g. contacts, mails) stored in your Microsoft Exchange Server and how you can restore them to your Microsoft Exchange Server from the backup files.

16.1 Requirements

Before you can perform Exchange Brick-Level Backup on your Quick Backup, please make sure that following requirements are met:

1. You are using one of the Microsoft Exchange Server listed in the Supported Listed.

2. Quick Backup must be installed on the computer running the Microsoft Exchange Server.

3. Install Microsoft Messaging Application Programming Interface (MAPI) on the computer running the Microsoft Exchange Server. In some cases, MAPI is installed with Microsoft Outlook.

4. For MS Exchange servers running on Windows SBS 2003/2008/2011 installations, the built-in administrator account is **must be enabled** (disabled by default).

5. The Windows account used to run the Exchange Brick-Level Backup on Quick Backup, for example administrator **must have a mailbox**.

6. Backup of Exchange 2010 SP1 in Hosting Mode is currently **not** supported.

Note:
Starting from Quick Backup version 6.5.4.0, it is now possible to run MS Exchange brick-level scheduled backups without changing the service logon for the Quick Backup scheduler service, from the default Local System account to the Domain Administrator account.

The Quick Backup scheduler service will automatically start the backup process (bJW.exe) using the windows user account defined in the backup setting "User Authentication for Windows". If "User Authentication for Windows" is not specified then the backup process (bJW.exe) will be run under using the Local System account. In this case, backup will usually fail with permission denied error.

16.2 Overview

Brick-Level Backup for Microsoft Exchange Server is not designed to fully protect an Exchange Server, but to facilitate easy backup and fast restore of individual emails, contacts, calendars, tasks etc.

The Brick-Level Restore cannot fully recover the Information Store after a disaster. If used, a Brick-Level Backup must be utilized in conjunction with full Information Store Backup, in order to fully protect the Exchange Server.

16.3 Granting Privileges

Brick-Level Backup requires "Full Mailbox Access" permission for the user running Quick Backup. Normally, Quick Backup can acquire the permission on its own but if you encounter “Access Denied" errors, you need to manually grant access privileges to the user running Quick Backup using one of the following instructions below:

For one specific mailbox

Use the following procedure to grant access to Exchange 2003 / 2007 mailbox:

1. Start [Active Directory Users and Computers].
2. On the [View] menu, ensure that the [Advanced Features] check box is selected.
3. Right click the user whose mailbox you want to give permissions to and choose [Properties].
4. On the [Exchange] Advanced tab, click [Mailbox Rights].
5. Notice that the Domain Admins and Enterprise Admins have both been given Deny access to Full Mailbox access.
6. Click [Add], click the user or group who you want to have access to this mailbox, and then click [OK].
7. Be sure that the user or group is selected in the Name box.
8. In the [Permissions] list, click [Allow] next to [Full Mailbox Access], and then click [OK].
9. Click [OK] all the way out.
10. Restart the Microsoft Exchange Information Store.

For mailboxes located within a specific mailbox store

Use the following procedure to grant access to Exchange 2003 / 2007 mailbox found on a specific mail store:

1. Start [Exchange System Manager].

2. Drill down to your server object within the appropriate Administrative Group. Expand the server object and find the required mailbox store within the appropriate Storage Group. Right click it and choose [Properties].

3. In the [Properties] window, go to the [Security] tab.

4. Click [Add], click the user or group who you want to have access to the mailboxes, and then click [OK].

5. Be sure that the user or group is selected in the Name box.

6. In the [Permission] list, check [Allow] next to [Full Control], and then click [OK].

7. Click [Apply] and [OK].

Restart the [Microsoft Exchange Information Store].

For mailboxes located within a specific server

For Exchange 2003, please follow the instructions below:

1. Add a new account that is a member of the "Domain Users" group and "Administrators" group to the Active Directory.

2. Right click [Exchange System Manager] -> [%DOMAIN_NAME%] -> [Server] -> [%EXCHANGE_SERVER_NAME%] and select [properties].

3. Choose the [Security] tab.

4. Add the new user to the list and then check the [Full Control] checkbox for this user.

5. Click [OK] all the way out.

6. Reboot the machine or restart [Microsoft Exchange Information service and wait 15 minutes for the changes to be fully applied to the Exchange Server.

For Exchange 2007, please follow the instructions below:

1. Create an account that is a member of local "Administrators", "Domain Admins", and "Enterprise Admins" groups.

2. Run the following command:

```
Get-MailboxServer | Add-ADPermission -User "%USER%" -AccessRights GenericAll -
  ExtendedRights ms-exch-store-admin,receive-as,send-as -InheritanceType All
```

For example, to grant the permission for the local account “system":

```
Get-MailboxServer | Add-ADPermission -User "System" -AccessRights GenericAll -
  ExtendedRights ms-exch-store-admin,receive-as,send-as -InheritanceType All
```

Other commands that may be useful:

Show added permission for a user account in AD

```
Get-MailboxServer | Get-ADPermission -User "%USER%"
```

For example:

```
Get-MailboxServer | Get-ADPermission -User "system"
```

Remove permission for a user account in AD

```
Get-MailboxServer | Remove-ADPermission -User "%USER%" -AccessRights GenericAll
  -ExtendedRights ms-exch-store-admin,receive-as,send-as -InheritanceType All
```

For example:

```
Get-MailboxServer | Remove-ADPermission -User "minimal" -AccessRights GenericAll -
  ExtendedRights ms-exch-store-admin,receive-as,send-as -InheritanceType All
```

For Exchange Server 2010, please do the followings:

1. Add a user account to the Exchange Server 2010 computer. This user account must be a member of the local "Administrators" (built-in), "Organization Management" (Microsoft Exchange Security Groups), "Domain Admins" and "Enterprise Admins" groups.

2. Please ensure that Update Rollup 3 for Exchange Server 2010 (KB981401) is installed on your machine.

3. Grant permission to a user by using the following command:

```
Get-Mailbox | Add-MailboxPermission -User "%USER%" -AccessRights FullAccess
```

For example:

```
Get-Mailbox | Add-MailboxPermission -User "SYSTEM" -AccessRights FullAccess
```

Other useful commands:

To remove AD permission:

```
Get-Mailbox | Remove-MailboxPermission -User "%USER%" -AccessRights FullAccess
```

For example:

```
Get-Mailbox | Remove-MailboxPermission -User "SYSTEM" -AccessRights FullAccess
```

To view the mailbox permission of a user:

```
Get-Mailbox | Get-MailboxPermission -User "%USER%"
```

For example:

```
Get-Mailbox | Get-MailboxPermission -User "SYSTEM"
```

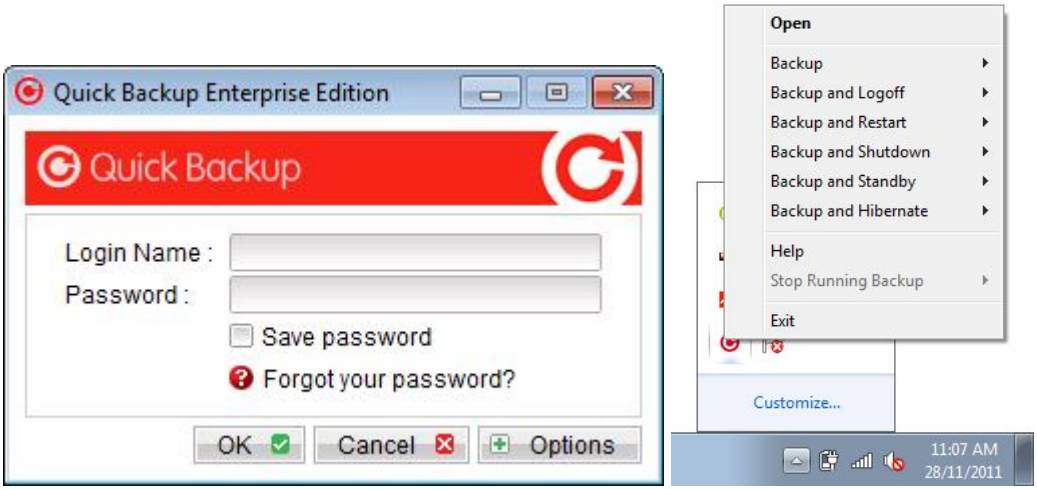
For details on how to troubleshoot for issue encountered when creating a mail level backup set, or during backup, please refer to
http://www.quickbackup.com.au/downloads/docs/How%20to%20troubleshoot%20MS%20Exchange%20mail%20level%20backup%20issue.pdf

16.4 How to perform Brick-Level backup

Refer to the follow instructions to backup individual items within your Microsoft Exchange Server:

1. Login to the backup application's user interface.

2.

3. 

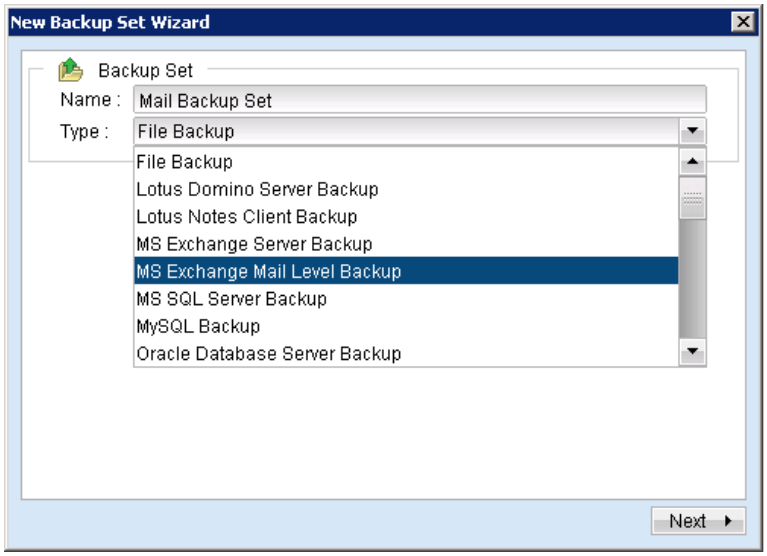
   For Quick Backup installation on 64 bit machines, please start the backup application by running the RunOBC32.bat file found under the application installation bin directory:

   ${Quick Backup-InstallHome}\bin\RunOBC32.bat

4. Select the [Backup Settings] button and the button to start the New Backup Set Wizard.

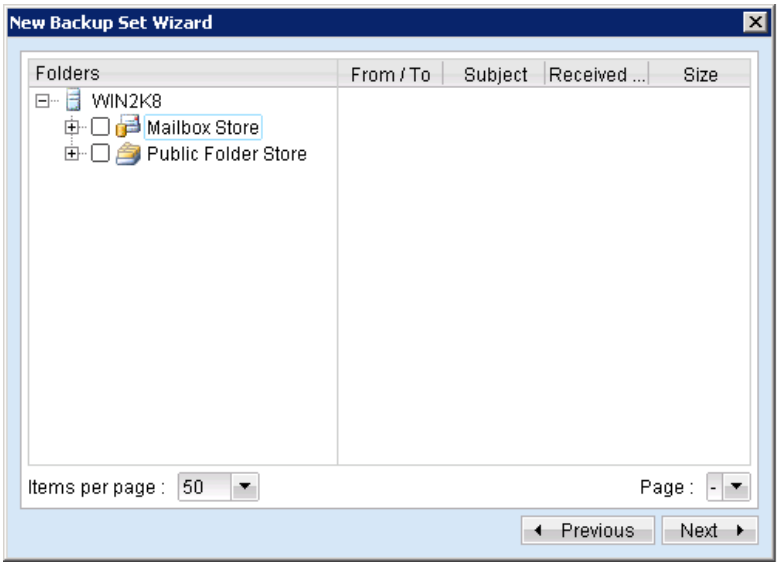
5. Create a MS Exchange mail level backup set by selecting [MS Exchange Mail Level Backup] from the backup set type dropdown menu.

6. Enter the backup set name



7. Select [Next] to proceed.

8. Expand the Mailbox Store to select the corresponding mailboxes for backup.



9. Configure a backup schedule for unattended backups.

10. Select an encryption setting for your backup set.

11. Press the [OK] button to complete the configuration of backup set.

12. Scheduled backup will run automatically if you leave your computer on.

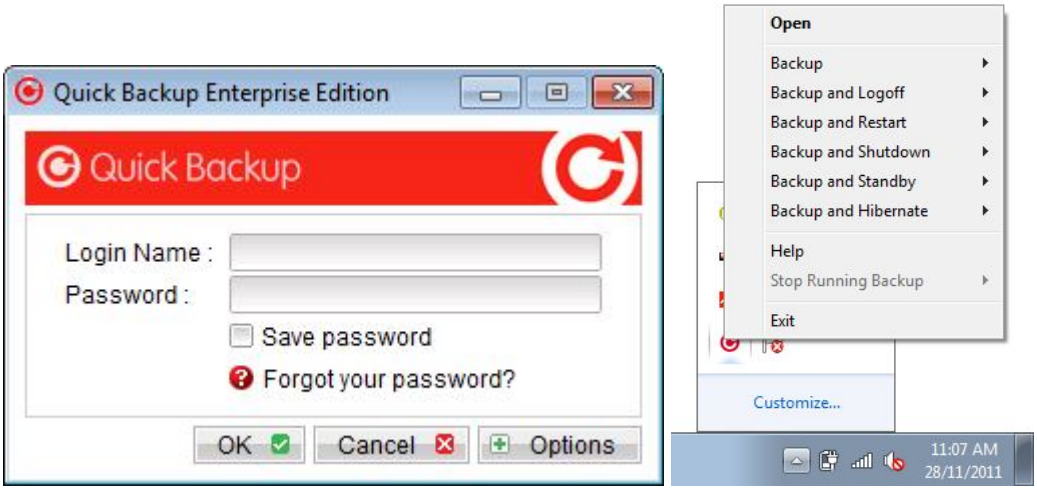
13. To perform a backup immediately, click [Backup] button on the left panel.

16.5 How to perform Brick-Level restore

Refer to the follow instructions to restore individual items to the original Microsoft Exchange Server

Note:
Please note that individual Brick-Level backup can only be restored using Quick Backup client (e.g. cannot perform web restore)

1. Login to the backup application's user interface.

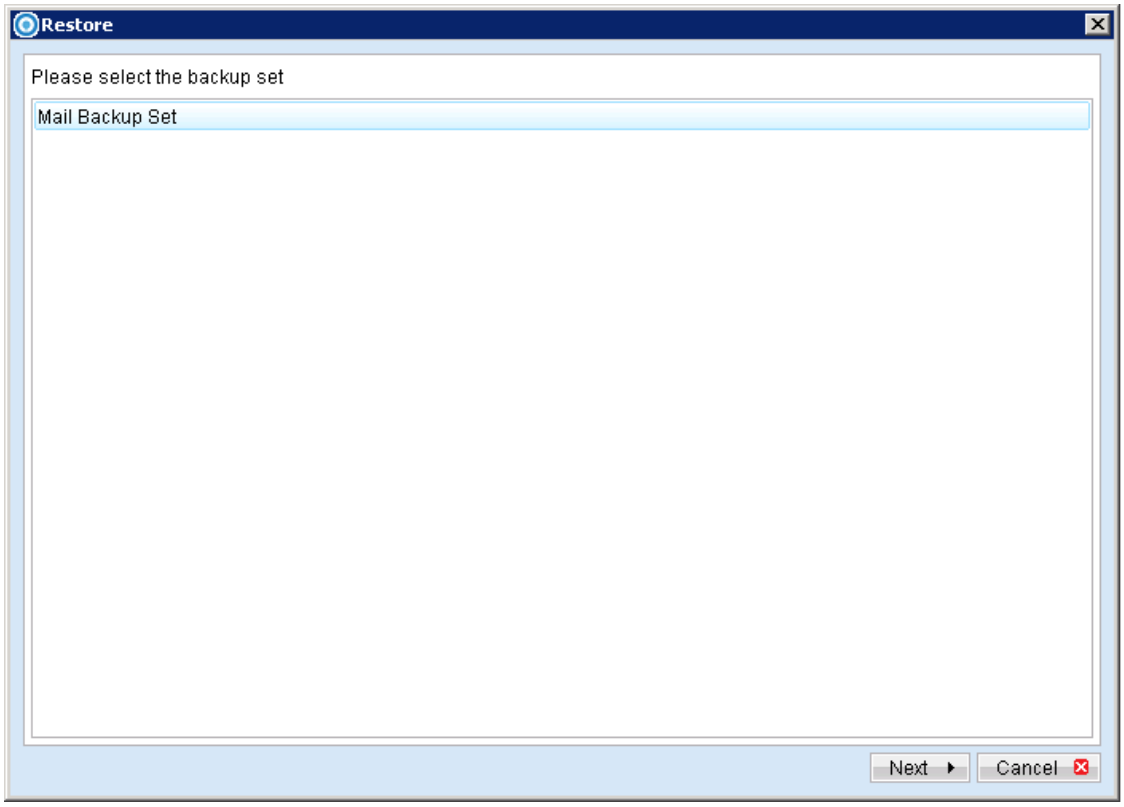


For Quick Backup installation on 64 bit machines, please start the backup application by running the RunOBC32.bat file found under the application installation bin directory:

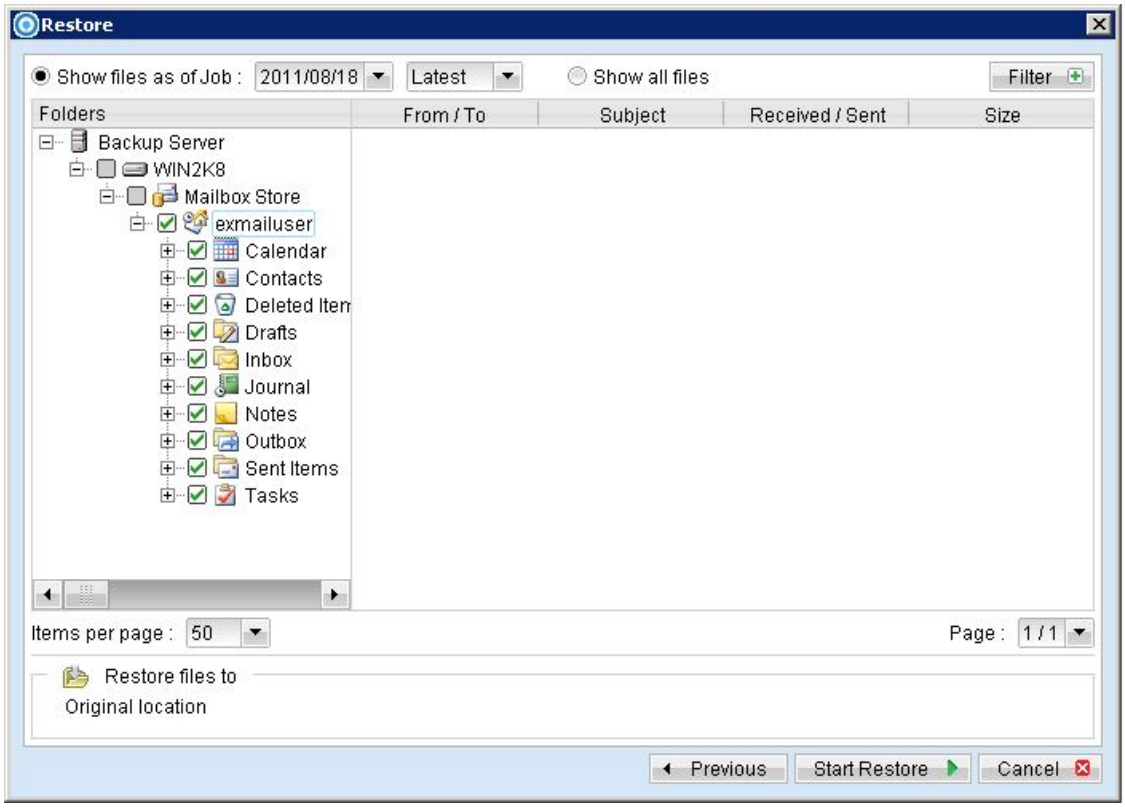
${Quick Backup-InstallHome}\bin\RunOBC32.bat

2. Select the [Restore] button on the Quick Backup main menu.

   Select the corresponding backup set to be restored.



3. Select the individual mail item to be restored.



4. Press the [Start Restore] button to restore.

17 Backup/Restore Oracle Database Server

This chapter will describe in details how Quick Backup backup your Oracle Database Server and how you can restore an Oracle database using the backup files.

17.1 Requirements

1. Quick Backup must be installed onto the computer that can connect to your Oracle Database Server using TCP/IP protocol.

2. Data from Oracle database will be backed up to a temporary directory before they are sent to Quick Backup Server. Please make sure you have sufficient space on your computer to store these data when you run the backup job.

3. Database must be in archived log mode.

   To switch database to archived log mode, please do the following:

   i. Set the parameters below in the PFILE to enable automatic archiving.

   ```
   LOG_ARCHIVE_DEST = <directory where archive redo logs will be stored>
   LOG_ARCHIVE_FORMAT = 'LOG%T_%S_%R.ARC'
   LOG_ARCHIVE_START = TRUE
   ```

   ii. Set ORACLE_SID to your database's System Identifier (SID):

   Windows

   ```
   Set ORACLE_SID=GDB1
   ```

   Linux

   ```
   export ORACLE_SID=GDB1 (assuming your database's SID is GDB1)
   ```

   iii. Run SQL Plus and connect to database as SYSDBA.

   For Oracle 9i/10g/11g

   ```
   SQLPLUS "/ as sysdba"
   ```

   For Oracle 8i

   ```
   connect internal;
   ```

iv. Shutdown database.

```
Shutdown immediate
```

v. Start and mount database.

```
startup mount
```

vi. Switch database to archived log mode.

```
alter database archivelog;
```

vii. Open database.

```
Alter database open;
```

Oracle 10g Example:

```
$ export ORACLE_SID=GDB1

$ sqlplus "/ as sysdba"

SQL*Plus: Release 10.2.0.1.0 - Production on Thu Nov 8 15:08:57 2007

Copyright (c) 1982, 2005, Oracle.  All rights reserved.


Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options

SQL> shutdown immediate
Database closed.
Database dismounted.
ORACLE instance shut down.

SQL> startup mount
ORACLE instance started.

Total System Global Area  285212672 bytes
Fixed Size                 1218992 bytes
Variable Size             96470608 bytes
Database Buffers         184549376 bytes
Redo Buffers               2973696 bytes
Database mounted.

SQL> alter database archivelog;

Database altered.

SQL> alter database open;
```

Database altered.

4. JAVASYSPRIV role is granted to system account.

   You can grant this role to system account by executing:

   Grant permission to system account.

   For Oracle 9i/10g/11g

SQL> grant javasyspriv to system;

   For Oracle 8i

SVRMGRL> connect internal *SVRMGRL> @?/javavm/instsall/initjvm.sql;* *SVRMGRL> @?/rdbms/admin/catalog.sql;* *SVRMGRL> @?/rdbms/admin/catproc.sql;* *SVRMGRL> @?/javavm/install/initdbj.sql;* *SQL> grant javasyspriv to system;*

Oracle 9i/10g/11g Example:
SQL? Grant javasyspriv to system; ***Grant succeeded.***

17.2 Overview

Quick Backup will backup your oracle database by taking the following steps.

1. Connect to the Oracle database using SQL*NET over TCP/IP.
2. Run all pre-Commands of this backup set.
3. If the backup type to run is [Database Backup Type],
    i. All data files in each of the tablespace(s) selected are copied to the temporary directory specified by this backup set.
    ii. If there are temporary files in the database, the script to re-create the temporary files are generated to a file located in the temporary directory specified by this backup set.
    iii. All non-default initialization parameters will be spooled to an initializing file located in the temporary directory specified by this backup set.
    iv. All control files will be copied to the temporary directory specified by this backup set.
    v. All archived log files will be copied to the temporary directory specified by this backup set.
4. If the backup type to run is [Archived Log Backup Type],
    i. All archived log files will be copied to the temporary directory specified by this backup set.
5. Run all Post-Commands of this backup set.
6. Upload all files copied to the temporary directory to Quick Backup Server.
7. Remove temporary files from the temporary directory.

Note:
If your Oracle database is running on Windows, please install Quick Backup onto the company running the Oracle database to backup this Oracle database. This would shorten the time required to backup the Oracle database.

17.3 How to backup an Oracle Database (Physical Backup)

Please follow the instructions below to backup your Oracle database to Quick Backup Server.

For Windows:

1. Install Quick Backup onto your computer.

2. Open Quick Backup.

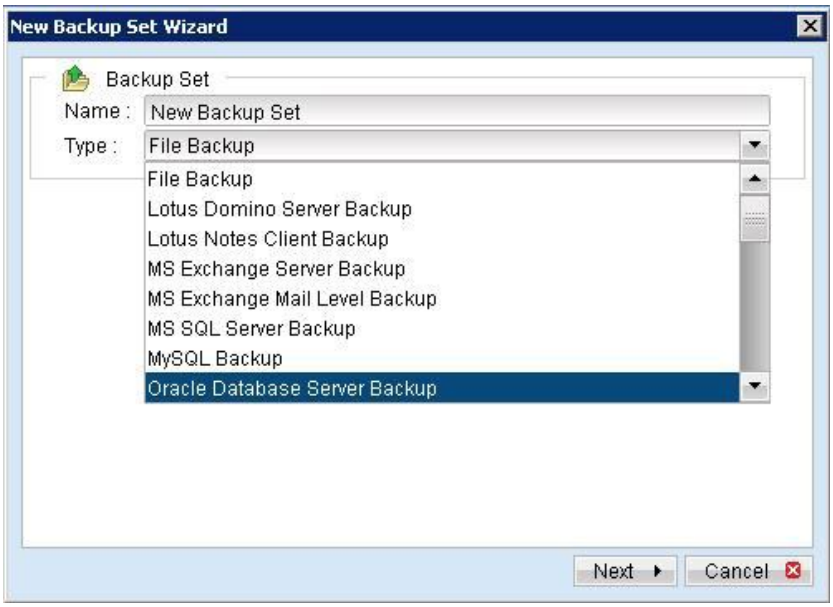
   Right click Quick Backup icon available in the system tray and choose [Open].

3. Create a backup set.

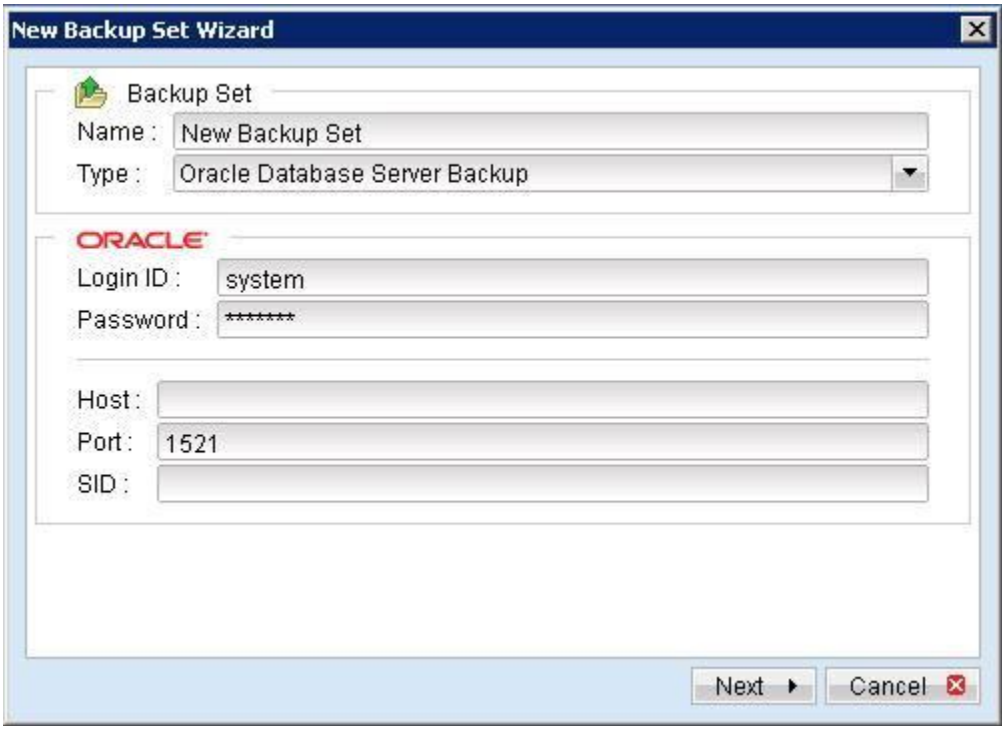
   i. To start setting up backup sets, click the button to open the [Backup Setting] dialog.

   ii. On the left panel, press the button to create a new backup set.

   iii. On the dialog, choose [Oracle Database Server Backup] as the [Type].

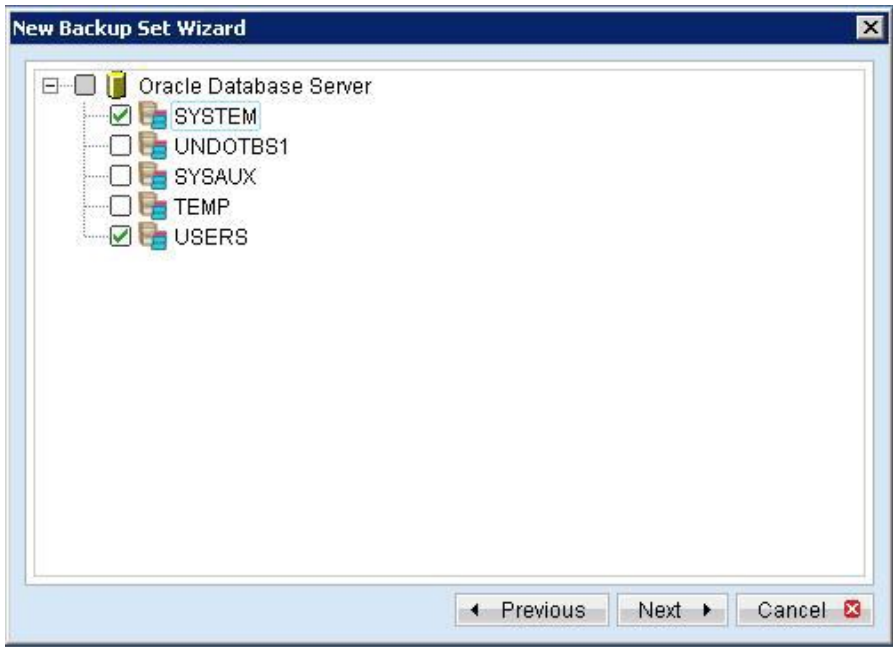


iv. Enter a name for your backup set.

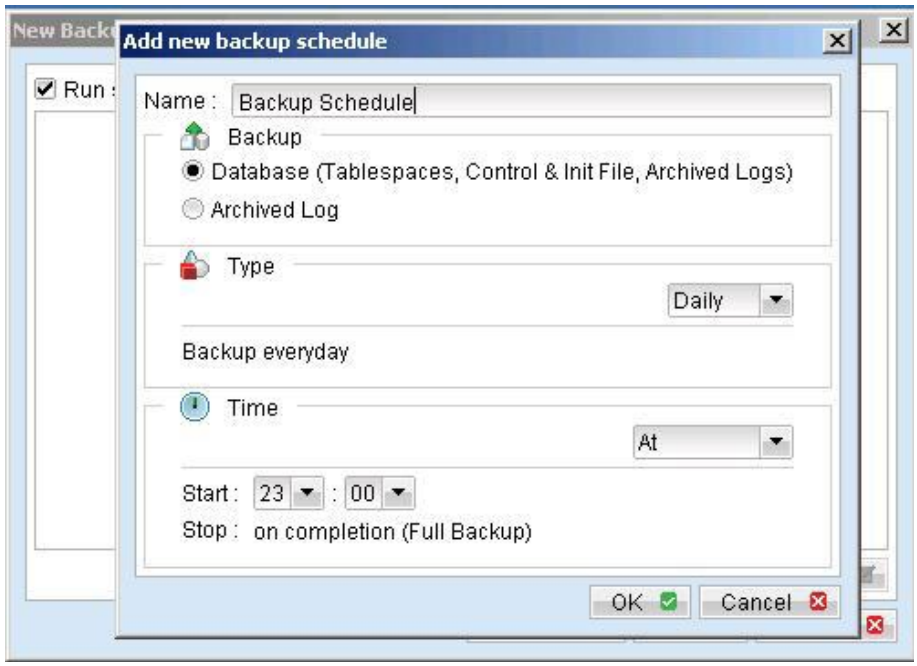


v. Enter the system password, the Oracle Database Server Host Name, TNS Port and SID.

vi. Select the tablespace(s) you want to backup.



vii. Set the backup schedule for database backup and archived log backup.



Note: You can have more than one schedule in a backup set, i.e. you can perform intra-day transaction log backup by adding more than one daily transaction log backup schedule to your backup set.

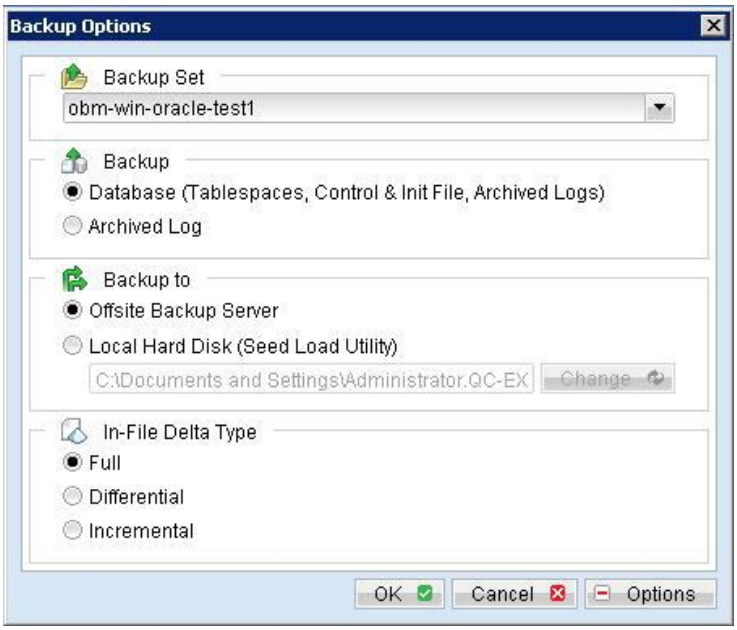
viii. Set the encryption algorithm, encryption mode and encryption key for this backup set.

Hint: For maximum security, please select AES (Advanced Encryption Standard) Algorithm, CBC (Cipher Block Chaining) mode and use an encrypting key with more than 8 characters.

4. Run Backup.

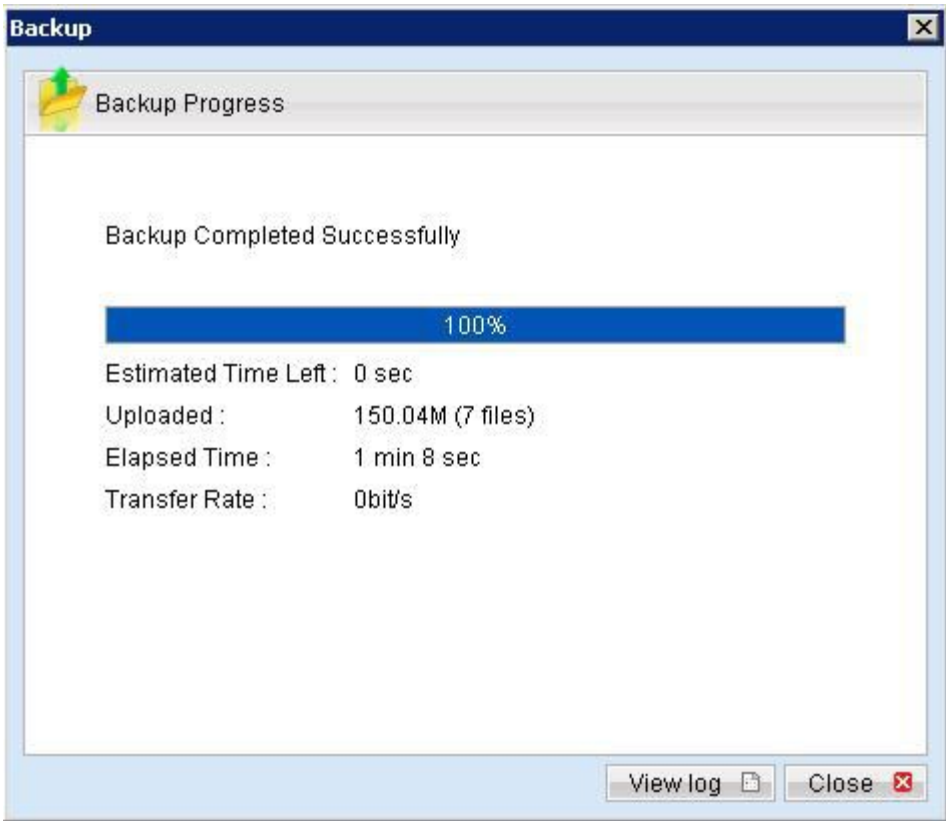
i. Press the [Backup] button on the main page of Quick Backup dialog.

ii. Select the backup type (e.g. Database Backup, Archived Log Backup) you would like to perform. Select the backup set you want to run and select [Offsite Backup Server] to start backing up your files to Quick Backup Server. If applicable, you can change the In-File Delta Type also.



iii. Click [OK] to start backing up your files to Quick Backup Server.

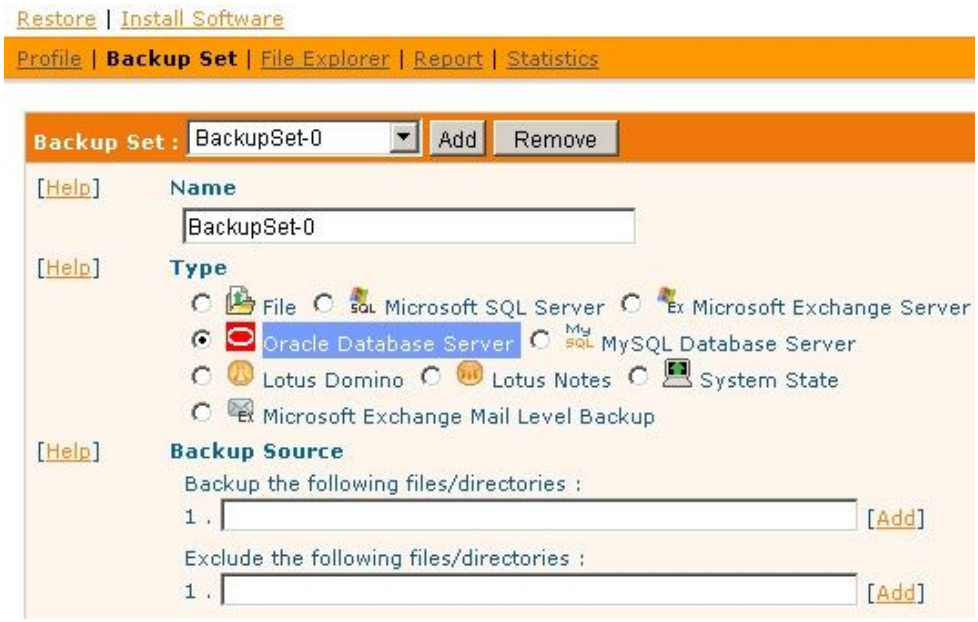
iv. When the backup finished, you should see the message “Backup Completed Successfully" as below.



For Linux

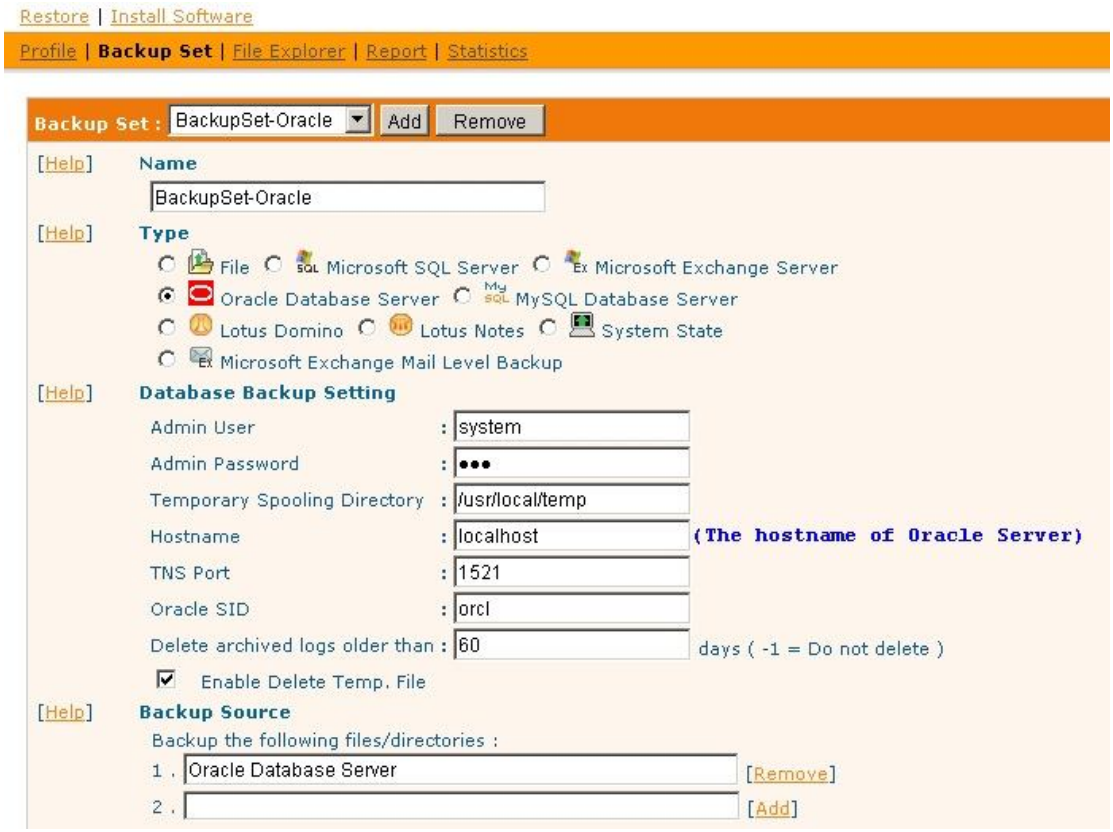
1. Install Quick Backup onto your Oracle Server.

2. Create a new backup set from Quick Backup Server web interface.



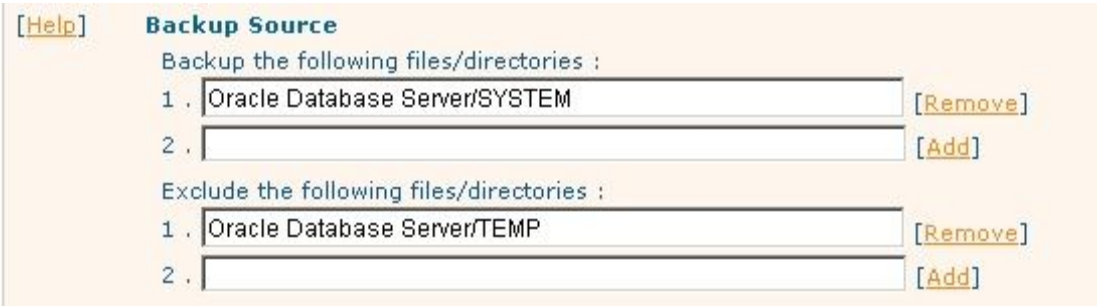
3. Select “Oracle Database Server" as the backup set type, then press [Update]. (You may also change the backup set’s Name at this stage).

4. Input the Database Backup Setting and the Backup Source.


Restore | Install Software
Profile | Backup Set | File Explorer | Report | Statistics
Backup Set : BackupSet-Oracle Add Remove
[Help] Name
BackupSet-Oracle
[Help] Type
File Microsoft SQL Server Microsoft Exchange Server
Oracle Database Server MySQL Database Server
Lotus Domino Lotus Notes System State
Microsoft Exchange Mail Level Backup
[Help] Database Backup Setting
Admin User : system
Admin Password : •••
Temporary Spooling Directory : /usr/local/temp
Hostname : localhost (The hostname of Oracle Server)
TNS Port : 1521
Oracle SID : orcl
Delete archived logs older than : 60 days (-1 = Do not delete)
Enable Delete Temp. File
[Help] Backup Source
Backup the following files/directories :
1 . Oracle Database Server [Remove]
2 . [Add]

5. Set the Backup Source as “Oracle Database Server" to backup all the table space.

6. You can also included or exclude a specific table space in your backup source. (E.g. Set the Backup Source as “Oracle Database Server/SYSTEM" to only backup the SYSTEM table space.) You may also set up the backup scheduled in this stage.

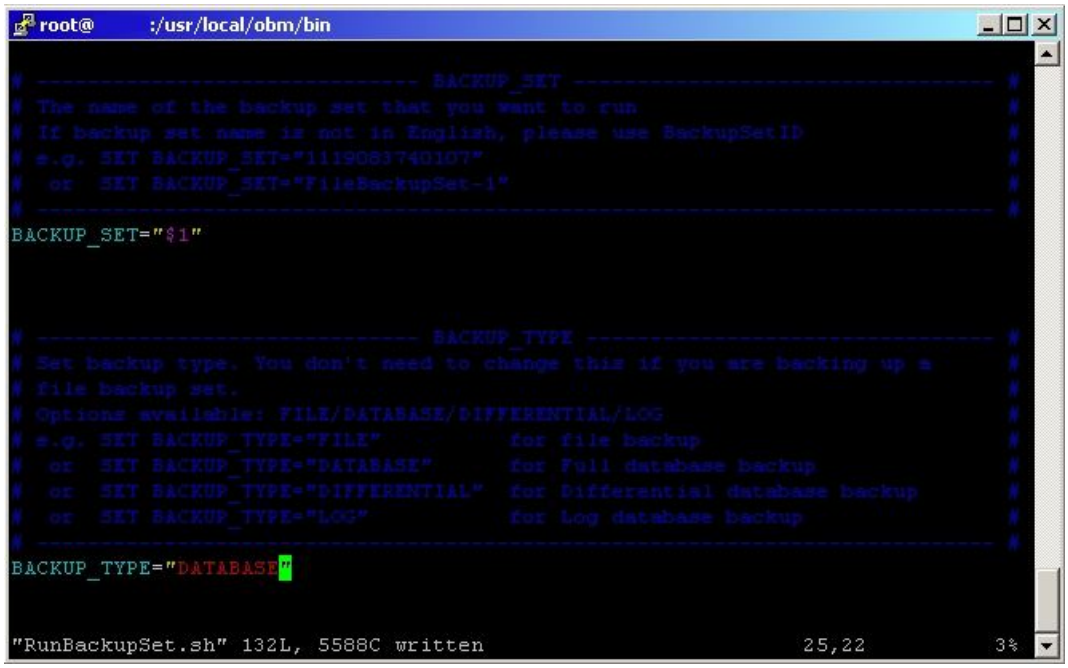

[Help] Backup Source
Backup the following files/directories :
1 . Oracle Database Server/SYSTEM [Remove]
2 . [Add]
Exclude the following files/directories :
1 . Oracle Database Server/TEMP [Remove]
2 . [Add]

7. If you intend to perform remote spool (Quick Backup install on a different machine from the Oracle Server). You may set the Hostname as the Oracle Server’s IP (e.g. Hostname: 192.168.101.109).

8. Logon to the Oracle Server machine and run $Quick Backup_HOME\bin\Configurator.sh to input the encryption key for the new backupset. You can also configure the backup set to run schedule backup on this computer at this stage.

9. The backup will run on schedule or you may perform a manual backup.

10. To perform manual backup, you will need to edit the script file $Quick Backup_HOME\bin\RunBackupSet.sh. Change the script from BACKUP_TYPE="FILE" to BACKUP_TYPE="DATABASE". Then save and exit the file.



11. Run the script file with the backup set name or ID as the parameter to perform a manual backup. (e.g. sh RunBackupSet.sh BackupSet-Oracle).

17.4 How to restore an Oracle Database

Please follow the instructions below to restore your Oracle 9i/10g/11/g database from Quick Backup Server.

1. Download the backup file from Quick Backup Server.

   Please refer to the Restoring Files section for information on how to download backup files from Quick Backup Server.

2. For restore an existing database.

   Shutdown the database.

   To shutdown the database, please do the following:

   i. Set ORACLE_SID to your database's System Identifier (SID):

      Windows

      > set ORACLE_SID=GDB1
      (Assuming your database's SID is GDB1)

      Linux

      $ export ORACLE_SID=GDB1
      (Assuming your database's SID is GDB1)

   ii. Run SQL Plus and connect to database as SYSDBA.

      $ sqlplus "/ as sysdba"

   iii. Shutdown database.

      SQL> shutdown immediate

Oracle 9i/10g/11g Example:
$ export ORACLE_SID=GDB1 **$ sqlplus "/ as sysdba"** **SQL*Plus: Release 10.2.0.1.0 – Production on Thu Nov 8 17:04:57 2007** **Copyright © 1982, 2005, Oracle. All right reserved.** **Connected to:** **Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 – Production** **With the Partitioning, OLAP and Data Mining options** **SQL> shutdown immediate** **Database closed.** **Database dismounted.** **ORACLE instance shut down.**

For recover a database that currently does not exist

Create a password file:

```
$ orapwd file=$ORACLE_HOME/dbs/orapwGDB1 password=pwd123
(assuming your database's SID is GDB1, and password is pwd123)
```

Oracle 9i/10g/11g Example:
$ orapwd file=/oracle/OraHome1/dbs/orapwBGDB1 password=pwd123

3. Put all downloaded backup files in place.

   Control files, data files and archived logs are stored on Quick Backup Server along with their full path information. You just need to put all these files back to their original locations when performing a database restore.

   For example:

```
/obm_restore/Oracle Database Server/oracle/product/10.2.0/db_1/admin/GDB1/
/obm_restore/Oracle Database Server/oracle/product/10.2.0/db_1/dbs/initGDB1.ora
/obm_restore/Oracle Database Server/oracle/product/10.2.0/db_1/dbs/spfileGDB1.ora
/obm_restore/Oracle Database
  Server/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1
/obm_restore/Oracle Database Server/oracle/product/10.2.0/db_1/oradata/GDB1
```

   Move to

```
/oracle/product/10.2.0/db_1/admin/GDB1/
/oracle/product/10.2.0/db_1/dbs/initGDB1.ora
/oracle/product/10.2.0/db_1/dbs/spfileGDB1.ora
/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/
/oracle/product/102.0/db_1/oradata/GDB1/
```

4. Rename database files (Only for restoring database to a new location).

   Rename your database files by doing the following:

   i. Modify the PFILE to update file path.

      Open the PFILE ($ORACLE_HOME/dbs/initGDB1.ora), change every file path to the new location, and then save it.

For example:

```
background_dump_dest = /oracle/OraHome1/admin/GDB2/bdump

control_files = (/oracle/OraHome1/oradata/GDB2/control01.ctl,
/oracle/OraHome1/oradata/GDB2/control02.ctl,
/oracle/OraHome1/oradata/GDB2/control03.ctl)

core_dump_dest = /oracle/OraHome1/admin/GDB2/cdump

user_dump_dest = /oracle/OraHome1/admin/GDB2/udump
```

Change to

```
background_dump_dest = /new_db_location/OraHome1/admin/GDB2/bdump

control_files = (/new_db_location/OraHome1/oradata/GDB2/control01.ctl,
/new_db_location/OraHome1/oradata/GDB2/control02.ctl,
/new_db_location/OraHome1/oradata/GDB2/control03.ctl)

core_dump_dest = /new_db_location/OraHome1/admin/GDB2/cdump

user_dump_dest = /new_db_location/OraHome1/admin/GDB2/udump
```

ii. You may need to quote the values of dispatchers as a single argument.

Add double quotation marks

Dispatchers = “(PROTOCOL=TCP) (SERVICE=GDB1XDB)"

iii. Delete the SPFILE.

Delete the SPFILE ($ORACLE_HOME/dbs/spfileGDB1/ora)

iv. Set ORACLE_SID to your database’s System identifier (SID).

Windows

```
> set ORACLE_SID=GDB1
(Assuming your database’s SID is GDB1)
```

Linux

```
$ export ORACLE_SID=GDB1
(Assuming your database’s SID is GDB1)
```

v. Run SQL Plus and connect to database as SYSDBA.

```
$ sqlplus "/ AS SYSDBA"
```

vi. Start and mount database.

```
SQL> startup mount
```

vii. Create a backup of the control file to trace file.

```
SQL>alter database backup controlfile to trace as
'New_DB_Location/CONTROL.TRC' reuse; (assuming you create a trace file to
/New_DB_Location/)
```

viii. Rename each of data file, log file and temp file.

Open the trace file that just created, and then check for the filename of each datafile, log file and tempfile.

Please do the following to rename each of the files:

```
SQL> ALTER DATABASE RENAME FILE 'xxx' TO 'YYY';

where xxx is the old filename found in the trace file, and yyy is the new filename
with updated path.
```

For example:

```
SQL> ALTER DATABASE RENAME FILE
'/oracle/product/10.2.0/db_1/oradata/GDB1/system01.dbf' TO
'/new_db_location/oradata/GDB1/system01.dbf';

SQL> ALTER DATABASE RENAME FILE
'/oracle/product/10.2.0/db_1/oradata/GDB1/undotbs01.dbf' TO
'/new_db_location/oradata/GDB1/undotbs01.dbf';

SQL> ALTER DATABASE RENAME FILE
'/oracle/product/10.2.0/db_1/oradata/GDB1/sysaux01.dbf' TO
'/new_db_location/oradata/GDB1/sysaux01.dbf';

SQL> ALTER DATABASE RENAME FILE
'/oracle/product/10.2.0/db_1/oradata/GDB1/users01.dbf' TO
'/new_db_location/oradata/GDB1/users01.dbf';

SQL> ALTER DATABASE RENAME FILE
'/oracle/product/10.2.0/db_1/oradata/GDB1/TS1' TO
'/new_db_location/oradata/GDB1/TS1';

SQL> ALTER DATABASE RENAME FILE
'/oracle/product/10.2.0/db_1/oradata/GDB1/redo01.log' TO
'/new_db_location/oradata/GDB1/redo01.log';
```

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/redo02.log' TO '/new_db_location/oradata/GDB1/redo02.log';

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/redo03.log' TO '/new_db_location/oradata/GDB1/redo03.log';

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/temp01.dbf' TO '/new_db_location/oradata/GDB1/temp01.dbf';

Oracle 9i/10g Example:

$ export ORACLE_STD=GDB1

$SQLPLUS "/ AS SYSDBA"

SQL*PLUS: Release 10.2.0.1.0 – Production on Fri Nov 9 17:50:30 2007

Copyright © 1982, 2005, Oracle. All rights reserved.

Connected to an idle instance.

SQL>startup mount

ORACLE instance started.

Total System Global Area 285212672 bytes
Fixed Size 1218992 bytes
Variable Size 92276304 bytes
Database Buffers 188743680 bytes
Redo Buffers 2973696 bytes
Database mounted.

SQL> alter database backup controlfile to trace as '/new_db_location/control.trc' reuse;

Database altered.

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/system01.dbf' TO '/new_db_location/oradata/GDB1/system01.dbf';

Database altered.

SQL> ALTER DATABASE RENAME FILE '/oracle/product/10.2.0/db_1/oradata/GDB1/undotbs01.dbf' TO '/new_db_location/oradata/GDB1/undotbs01.dbf';

Database altered.

```
SQL> ALTER DATABASE RENAME FILE
'/oracle/product/10.2.0/db_1/oradata/GDB1/sysaux01.dbf' TO
'/new_db_location/oradata/GDB1/sysaux01.dbf';

Database altered.

SQL> ALTER DATABASE RENAME FILE
'/oracle/product/10.2.0/db_1/oradata/GDB1/users01.dbf' TO
'/new_db_location/oradata/GDB1/users01.dbf';

Database altered.

SQL> ALTER DATABASE RENAME FILE
'/oracle/product/10.2.0/db_1/oradata/GDB1/TS1' TO
'/new_db_location/oradata/GDB1/TS1';

Database altered.

SQL> ALTER DATABASE RENAME FILE
'/oracle/product/10.2.0/db_1/oradata/GDB1/redo01.log' TO
'/new_db_location/oradata/GDB1/redo01.log';

Database altered.

SQL> ALTER DATABASE RENAME FILE
'/oracle/product/10.2.0/db_1/oradata/GDB1/redo02.log' TO
'/new_db_location/oradata/GDB1/redo02.log';

Database altered.

SQL> ALTER DATABASE RENAME FILE
'/oracle/product/10.2.0/db_1/oradata/GDB1/redo03.log' TO
'/new_db_location/oradata/GDB1/redo03.log';

Database altered.

SQL> ALTER DATABASE RENAME FILE
'/oracle/product/10.2.0/db_1/oradata/GDB1/temp01.dbf' TO
'/new_db_location/oradata/GDB1/temp01.dbf';

Database altered.
```

5. Restore Database.

Use Recovery Manager to restore your database by doing the following:

For Oracle 9i/10g/11g

i. Set ORACLE_SID to your database's System Identifier (SID).

Windows

```
> set ORACLE_SID=GDB1
(Assuming your database's SID is GDB1)
```

Linux

```
$ export ORACLE_SID=GDB1
(Assuming your database's SID is GDB1)
```

ii. Run Oracle Recovery Manager (rman) and connect to the target database.

```
$rman target /
```

iii. Start and mount database.

```
RMAN> startup mount
```

iv. Reapply all transactions from the archived log files to the last sequence.

```
RMAN> recover database until sequence=4 thread=1; (assuming the sequence number of your last archived redo log is 3
```

Sequence numbers are named on the filename of archived redo log.

e.g.

/oracle/OraHome1/dbs/ol_mf_1_2_3m5hlsvs_.arc

/oracle/OraHome1/dbs/ol_mf_1_3_3m5hlyby_.arc

In this case, the sequence number of archived redo log is 4.

v. Open database

```
RMAN> alter database open resetlogs;
```

Oracle 9i/10g/11g Example
$ export ORACLE_SID=GDB1 ***$ rman target /*** ***Recovery Manager: Release 10.2.0.1.0 - Production on Thu Nov 8 17:46:27 2007***

Copyright (c) 1982, 2005, Oracle. All rights reserved.

connected to target database (not started)

RMAN> startup mount

Oracle instance started
database mounted

Total System Global Area 285212672 bytes

Fixed Size 1218992 bytes
Variable Size 113247824 bytes
Database Buffers 167772160 bytes
Redo Buffers 2973696 bytes

RMAN> recover database until sequence=4 thread=1;

Starting recover at 08-NOV-07
Starting implicit crosscheck backup at 08-NOV-07
using target database control file instead of recovery catalog
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=157 devtype=DISK
Finished implicit crosscheck backup at 08-NOV-07

Starting implicit crosscheck copy at 08-NOV-07
using channel ORA_DISK_1
Finished implicit crosscheck copy at 08-NOV-07

searching for all files in the recovery area
cataloging files...
cataloging done

List of Cataloged Files
==========
File Name:
/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/archivelog/2007_11_08/o1_mf_1_3_3m5h1yby_.arc

using channel ORA_DISK_1

starting media recovery

archive log thread 1 sequence 2 is already on disk as file
/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/archivelog/2007_11_08/o1_mf_1_2_3m5h1svs_.arc
archive log thread 1 sequence 3 is already on disk as file
/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/archivelog/2007_11_08/o1_mf_1_3_3m5h1yby_.arc
archive log
filename=/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/archivelog/2007_11_08/o1_mf_1_2_3m5h1svs_.arc thread=1 sequence=2
archive log
filename=/oracle/product/10.2.0/db_1/flash_recovery_area/GDB1/archivel

```
og/2007_11_08/o1_mf_1_3_3m5h1yby_.arc thread=1 sequence=3
media recovery complete, elapsed time: 00:00:01
Finished recover at 08-NOV-07

RMAN> alter database open resetlogs;

database opened
```

For Oracle 8i

i. Set ORACLE_SID to your database's System Identifier (SID).

ii. Run Oracle Server Manager. (svrmgrl)

Windows

```
> set ORACLE_SID=GDB1
(Assuming your database's SID is GDB1)
> svrmgrl
```

Linux

```
$ export ORACLE_SID=GDB1
(Assuming your database's SID is GDB1)
$ svrmgrl
```

iii. Connect to the target database.

```
SVRMGRL> connect internal
```

iv. Start and mount database.

```
SVRMGRL> start mount;
```

v. Reapply all transactions from the archived log files.

```
RMAN> recover database using backup controlfile
```

vi. Open database.

```
RMAN> ALTER DATABASE OPEN RESETLOGS;
```

Oracle 8i Example:

```
$ svrmgrl

SVRMGRL> connect internal

SVRMGR> startup mount;
ORACLE instance started.
Total System Global Area                    958744
Fixed Size
Variable Size
Database Buffers
Redo Buffers
Database mounted.

SVRMGRL> recover database using backup controlfile
ORA-00279: change 419671 generated at 06/14/03 02:51:49 needed for
```

```
thread 1
ORA-00289: suggestion : /data/ora815/vin/archive/ARCH0000000225.LOG
ORA-00280: change 419671 for thread 1 is in sequence #225
ORA-00278: log file '/data/ora815/vin/archive/ARCH0000000224.LOG' no
longer needed for this recovery
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
AUTO
Log applied.
. . . . . .
ORA-00279: change 547222 generated at 06/18/03 19:58:26 needed for
thread 1
ORA-00289: suggestion : /data/ora815/vin/archive/ARCH0000000384.LOG
ORA-00280: change 547222 for thread 1 is in sequence #384
ORA-00278: log file '/data/ora815/vin/archive/ARCH0000000383.LOG' no
longer needed for this recovery
ORA-00308: cannot open archived log
'/data/ora815/vin/archive/ARCH0000000384.LOG'
ORA-27037: unable to obtain file status
Linux Error: 2: No such file or directory
Additional information: 3

SVRMGR> recover database using backup controlfile until cancel
ORA-00279: change 547222 generated at 06/18/03 19:58:26 needed for
thread 1
ORA-00289: suggestion : /data/ora815/vin/archive/ARCH0000000384.LOG
ORA-00280: change 547222 for thread 1 is in sequence #384
Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
CANCEL
Media recovery cancelled.
SVRMGR> alter database open resetlogs;
Statement processed.
```

6. (Optional) Create Net Service Name and Database Service Listener.

   To create Net Service Name

   Start Net Manager by running the command netmgr

```
$ netmgr
```

   i. Expand [Oracle Net Configuration].

   ii. Expand [Local].

   iii. Select [Service Naming].

   iv. Click “+" icon on the toolbar.

   v. Net Service Name wizard will be launched to guide you through creating a net service name.

   vi. Click [File] on the menu bar.

   vii. [Save Network Configuration] on the menu bar.

To create Database Service Listener

Start Net Manager by running the command netmgr

```
$ netmgr
```

i. Expand [Oracle Net Configuration].

ii. Expand [Local].

iii. Expand [Listeners].

iv. Select [LISTENER]

v. Select [Database Services] from combo box.

vi. Click [Add Database].

vii. Input Global Database Name and SID.

viii. Click [File] on the menu bar.

ix. [Save Network Configuration] on the menu bar.

17.5 How to restore a single tablespace

Restoring a tablespace required a backup of datafiles consistent with the existing archived logs and control files, as redo will be applied during the restore operation.

Please follow the instructions below to restore a tablespace from Quick Backup Server.

1. Download the backup files from Quick Backup Server.

   Please refer to the Restoring Files section for information on how to download backup files from Quick Backup Server.

2. Set ORACLE_SID to your database's System Identifier (SID).

   Windows

```
> set ORACLE_SID=GDB1
(Assuming your database's SID is GDB1)
```

   Linux

```
$ export ORACLE_SID=GDB1
(Assuming your database's SID is GDB1)
```

3. Run SQL Plus and connect to database as SYSDBA.

```
$ SQLPLUS "/ as sysdba"
```

4. Shutdown database.

```
SQL> shutdown immediate
```

5. Put the downloaded tablespace datafiles in place.

   Datafile names and paths can be found by using the REPORT SCHEMA command.

   i. Set ORACLE_SID to your database's System Identifier (SID).

```
$ export ORACLE_SID=GDB1 (assuming your database's SID is GDB1)
```

   ii. Run Oracle Recovery Manager (rman) and connect to target database.

```
$ rman target /
```

   iii. Start and mount database

```
RMAN> startup mount
```

   iv. List the names of all datafiles and tablespaces.

```
RMAN> report schema;
```

   For example:

```
Report of database schema
File K-bytes    Tablespace  RB segs Datafile Name
---- ---------- ----------- ------- ------------------
1       419840 SYSTEM      ***
/oracle/OraHome1/oradata/GDB1/system01.dbf
2       204800 UNDOTBS1    ***
/oracle/OraHome1/oradata/GDB1/undotbs01.dbf
3        20480 CWMLITE     ***
/oracle/OraHome1/oradata/GDB1/cwmlite01.dbf
4        20480 DRSYS       ***     /oracle/OraHome1/oradata/GDB1/drsys01.dbf
5       141440 EXAMPLE     ***
/oracle/OraHome1/oradata/GDB1/example01.dbf
6        25600 INDX        ***     /oracle/OraHome1/oradata/GDB1/indx01.dbf
7        20480 ODM         ***     /oracle/OraHome1/oradata/GDB1/odm01.dbf
8        10240 TOOLS       ***     /oracle/OraHome1/oradata/GDB1/tools01.dbf
9        25600 USERS       ***     /oracle/OraHome1/oradata/GDB1/users01.dbf
10       39040 XDB         ***     /oracle/OraHome1/oradata/GDB1/xdb01.dbf
11           0 TS1         ***     /oracle/OraHome1/oradata/GDB1/TS1_datafile1.dbf
12           0 TS1         ***     /oracle/OraHome1/oradata/GDB1/TS1_datafile2.dbf
13           0 TS1         ***     /oracle/OraHome1/oradata/GDB1/TS1_datafile3.dbf
```

v. Put all the downloaded backup of datafile/s that constitute the tablespace to the listed location.

For example:

```
/obm_restore/Oracle Database
Server/oracle/OraHome1/oradata/GDB1/TS1_datafile1.dbf

/obm_restore/Oracle Database
Server/oracle/OraHome1/oradata/GDB1/TS1_datafile2.dbf

/obm_restore/Oracle Database
Server/oracle/OraHome1/oradata/GDB1/TS1_datafile3.dbf
```

Move to

```
/oracle/OraHome1/oradata/GDB1/TS1_datafile1.dbf

/oracle/OraHome1/oradata/GDB1/TS1_datafile2.dbf

/oracle/OraHome1/oradata/GDB1/TS1_datafile3.dbf
```

6. Restore tablespace.

```
RMAN> recover tablespace TS1; (assuming your tablespace is TS1)
```

If your datafiles is consistent with the database, you should see:

Oracle 9i/10g Example:

```
RMAN> recover tablespace TS1;
```

```
Starting recover at 19-JUL-07
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=156 devtype=DISK

starting media recovery

archive log thread 1 sequence 1 is already on disk as file
D:\ORACLE\PRODUCT\10.
2.0\FLASH_RECOVERY_AREA\GDB1\ARCHIVELOG\2007_07_19\O1_MF_1_1
_39Y98F0H_.ARC
archive log thread 1 sequence 2 is already on disk as file
D:\ORACLE\PRODUCT\10.
2.0\FLASH_RECOVERY_AREA\GDB1\ARCHIVELOG\2007_07_19\O1_MF_1_2
_39Y98JSD_.ARC
archive log thread 1 sequence 3 is already on disk as file
D:\ORACLE\PRODUCT\10.
2.0\FLASH_RECOVERY_AREA\GDB1\ARCHIVELOG\2007_07_19\O1_MF_1_3
_39Y9SW4D_.ARC
archive log
filename=D:\ORACLE\PRODUCT\10.2.0\FLASH_RECOVERY_AREA\GDB1\AR
CHIVELO
G\2007_07_19\O1_MF_1_1_39Y98F0H_.ARC thread=1 sequence=1
media recovery complete, elapsed time: 00:00:01
Finished recover at 19-JUL-07
```

If your datafiles does not consistent with the database, you should see:

Oracle 9i/10g Example:

```
RMAN> recover tablespace TS1;

Starting recover at 19-JUL-07
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=156 devtype=DISK
RMAN-00571:
===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS
===============
RMAN-00571:
===========================================================
RMAN-03002: failure of recover command at 07/20/2007 12:24:49
RMAN-06163: some datafiles cannot be recovered, aborting the RECOVER
command
RMAN-06166: datafile 7 cannot be recovered
RMAN-06166: datafile 6 cannot be recovered
RMAN-06166: datafile 5 cannot be recovered
```

In this case, you need to find the consistent datafiles in order to restore the tablespace.

If there are archive log missing, you should see:

Oracle 9i/10g Example:

```
RMAN> recover tablespace TS1;

Starting recover at 20-JUL-07
```

```
using channel ORA_DISK_1

starting media recovery

archive log thread 1 sequence 12 is already on disk as file
D:\ORACLE\PRODUCT\10
.2.0\FLASH_RECOVERY_AREA\GDB1\ARCHIVELOG\2007_07_18\O1_MF_1_1
2_39VF4JNJ_.ARC
RMAN-00571:
===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS
===============
RMAN-00571:
===========================================================
RMAN-03002: failure of recover command at 07/20/2007 12:28:52
RMAN-06053: unable to perform media recovery because of missing log
RMAN-06025: no backup of log thread 1 seq 13 lowscn 660617 found to
restore
```

In this case, you need to find the missing archive log files in order to restore the tablespace.

7. Open database.

RMAN> alter database open;

Oracle 9i/10g Example:

```
$ export ORACLE_SID=GDB1

$ rman target /

Recovery Manager: Release 9.2.0.1.0 - Production

Copyright (c) 1995, 2002, Oracle Corporation.  All rights reserved.

connected to target database (not started)

RMAN> startup mount

Oracle instance started
database mounted

Total System Global Area     235999352 bytes

Fixed Size                     450680 bytes
Variable Size                201326592 bytes
Database Buffers              33554432 bytes
Redo Buffers                    667648 bytes

RMAN> report schema;

using target database control file instead of recovery catalog
Report of database schema

using target database controlfile instead of recovery catalog
```

```
Report of database schema
File K-bytes    Tablespace         RB segs Datafile Name
---- ---------- ------------------ ------- ------------------
1       419840 SYSTEM             ***
/oracle/OraHome1/oradata/GDB1/system01.dbf
2       204800 UNDOTBS1           ***
/oracle/OraHome1/oradata/GDB1/undotbs01.dbf
3        20480 CWMLITE            ***
/oracle/OraHome1/oradata/GDB1/cwmlite01.dbf
4        20480 DRSYS              ***
/oracle/OraHome1/oradata/GDB1/drsys01.dbf
5       141440 EXAMPLE            ***
/oracle/OraHome1/oradata/GDB1/example01.dbf
6        25600 INDX               ***     /oracle/OraHome1/oradata/GDB1/indx01.dbf
7        20480 ODM                ***     /oracle/OraHome1/oradata/GDB1/odm01.dbf
8        10240 TOOLS              ***
/oracle/OraHome1/oradata/GDB1/tools01.dbf
9        25600 USERS              ***
/oracle/OraHome1/oradata/GDB1/users01.dbf
10       39040 XDB                ***     /oracle/OraHome1/oradata/GDB1/xdb01.dbf
11           0 TS1                ***
/oracle/OraHome1/oradata/GDB1/TS1_datafile1.dbf
12           0 TS1                ***
/oracle/OraHome1/oradata/GDB1/TS1_datafile2.dbf
13           0 TS1                ***
/oracle/OraHome1/oradata/GDB1/TS1_datafile3.dbf

List of Temporary Files
=======================
File Size(MB) Tablespace         Maxsize(MB) Tempfile Name
---- -------- -------------------- ----------- --------------------
1    20       TEMP                 32767       D:\ORACLE\PRODUCT\10.2.0\ORADATA\
GDB1\TEMP01.DBF

RMAN> recover tablespace TS1;

Starting recover at 30-AUG-07
allocated channel: ORA_DISK_1
channel ORA_DISK_1: sid=11 devtype=DISK

starting media recovery
media recovery complete

Finished recover at 30-AUG-07

RMAN> alter database open;

database opened
```

17.6 Export and Import a Database (Logical Backup)

While physical backup of database file permit the full reconstruction of database, logical backup is a useful supplement to physical backup for some purposes. For instance, logical backup using the export and import utilities are the only method that Oracle supports for moving an existing database from one platform to another.

Please follow the instructions below to backup a database:

1. Export the full database to a dump file.

```
$ exp system/pwd123 FULL=y FILE='/oracle/data.dmp' LOG='/oracle/export.log'
```

(Assuming your system password is pwd123, the name of dump file is /oracle/data.dmp and the name of log file is /oracle/export.log)

Oracle 9i/10g Example:

```
$ exp system/pwd123 FULL=y FILE='/oracle/data.dmp'
LOG='/oracle/export.log'

Connected to: Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 -
Production
With the Partitioning, OLAP and Data Mining options
Export done in WE8MSWIN1252 character set and AL16UTF16 NCHAR
character set

About to export the entire database ...
. exporting tablespace definitions
. exporting profiles
. exporting user definitions
. exporting roles
. exporting resource costs

                    //////////////////////
                    // ... exporting ... //
                    //////////////////////

. exporting dimensions
. exporting post-schema procedural objects and actions
. exporting user history table
. exporting default and system auditing options
. exporting statistics
Export terminated successfully without warnings.
```

2. Backup the exported dump file to Quick Backup Server.

Please refer to the [Section 6.2 Backup Files directly to the backup server] for information on how to upload backup files to Quick Backup Server.

Please follow the instructions below to restore a database:

1. Download the backup files from Quick Backup Server.

   Please refer to the Section 8 for information on how to download backup files from Quick Backup Server.

2. Import the full database from the downloaded backup of dump file.

$ imp system/pwd123 FULL=y FILE='/oracle/data.dmp' LOG='/oracle/import.log'
(assuming your system password is pwd123, the name of dump file is .oracle/data.dmp and the name of log file is /oracle/import.log)

Oracle 9i/10g Example:

$ imp system/pwd123 FULL=y FILE='/oracle/data.dmp' LOG='/oracle/import.log'

Connected to: Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options

Export file created by EXPORT:V10.02.01 via conventional path
import done in WE8MSWIN1252 character set and AL16UTF16 NCHAR character set
. importing SYSTEM's objects into SYSTEM
. importing OLAPSYS's objects into OLAPSYS
. importing SYSMAN's objects into SYSMAN
. importing SYSTEM's objects into SYSTEM
. importing OLAPSYS's objects into OLAPSYS

//////////////////////
// ... importing ... //
//////////////////////

. importing OLAPSYS's objects into OLAPSYS
. importing SYSTEM's objects into SYSTEM
. importing OLAPSYS's objects into OLAPSYS
. importing SYSMAN's objects into SYSMAN
. importing SCOTT's objects into SCOTT
Import terminated successfully without warnings.

18 Backup/Restore Microsoft SQL Server

This chapter describes in details how to use Quick Backup to backup your Microsoft SQL Server 2005 /2008 and how to restore your Microsoft SQL 2005/ 2008 server from the backup files.

18.1 Requirements

1. Quick Backup must be installed onto the computer running Microsoft SQL Server.

2. Data from Microsoft SQL Server will be backed up to a temporary directory before they are sent to Quick Backup Server. Please make sure you have sufficient space on your computer to store these data when you run the backup job.

18.2 Overview

Quick Backup will backup your Microsoft SQL Server database(s) by taking the following steps:

1. Before running any backup activities, Quick Backup will run all Pre-Commands of the backup set.

2. For each database that is to be backed up, Quick Backup will issue a database / transaction log backup command to Microsoft SQL Server to backup each database to a Microsoft SQL Server database backup file (*.bak file) and save it in the temporary directory you specified.

3. After all *.bak files have been spooled to the temporary directories, Quick Backup will run all Post-Commands of the backup set.

4. Upload all files copied to the temporary directory to Quick Backup Server.

5. Remove temporary files from the temporary directory.

18.3 How to backup Microsoft SQL Server database(s)

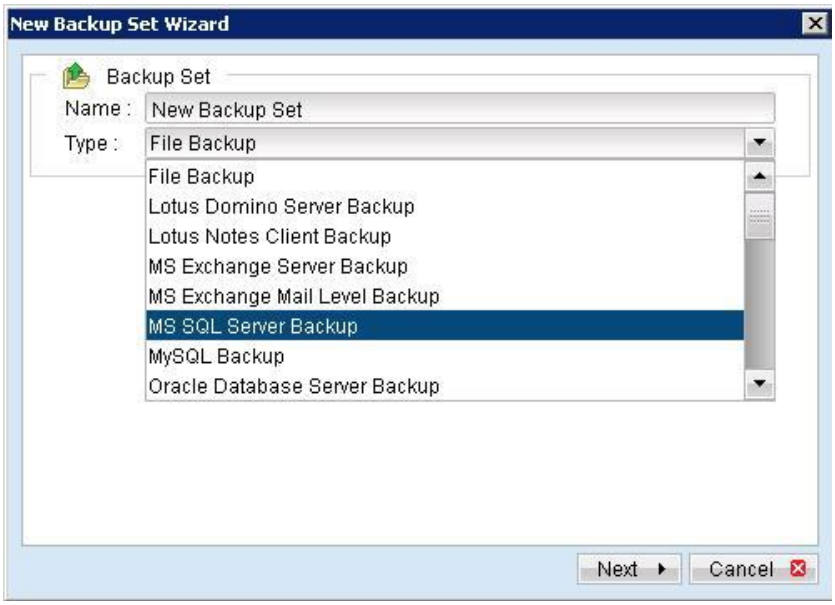
1. Open Quick Backup and right click Quick Backup icon available in the system tray and choose [Open].

2. Create a backup set.

   i. To start setting up backup sets, click the button to open the [Backup Setting] dialog.

   ii. On the left panel, press the button to create a new backup set.

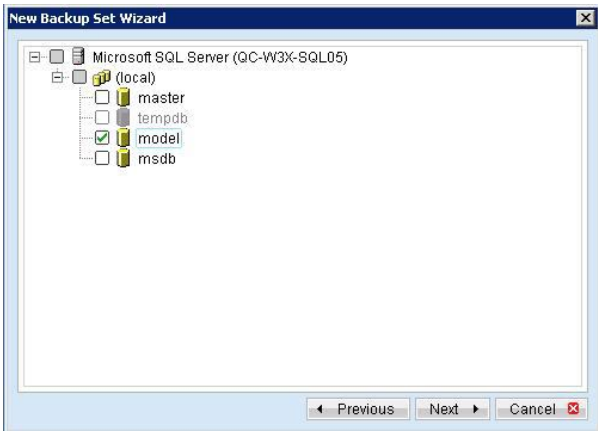
   iii. On the dialog, choose [MS SQL Server Backup] as the [Type].



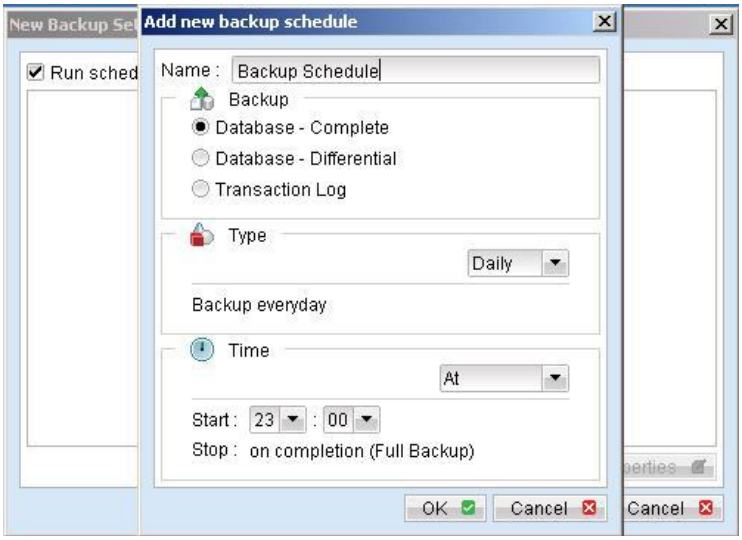
   iv. Enter a name for your backup set.

   v. Enter the Microsoft SQL Server administrator username and password.

   vi. Select the database(s) you want to backup.

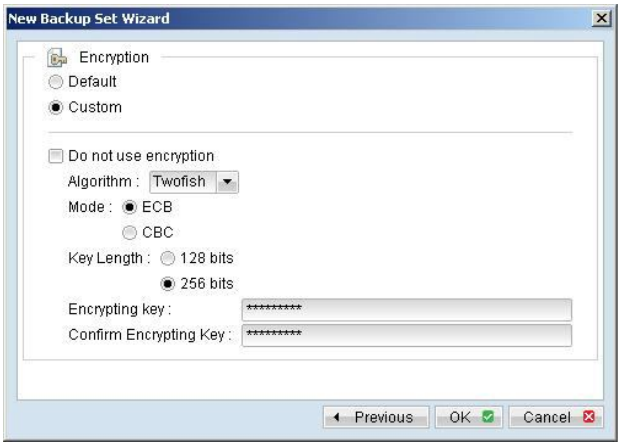


vii. Set the backup schedule for full database backup and transaction log backup.



(Note: You can have more than one schedule in a backup set, i.e. you can perform intra-day transaction log backup by adding more than one daily transaction log backup schedule to your backup set).

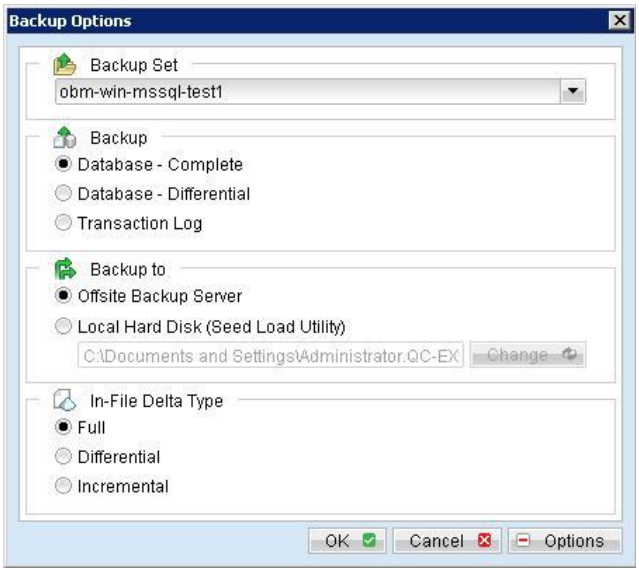
viii. Set the encryption algorithm, encryption mode and encrypting key for this backup set.



3. Run Backup

i. Press the [Backup] button on the main page of Quick Backup dialog.

ii. Select the backup type (e.g. Complete, Differential, and Transaction Log) you would like to perform. Select the backup set you want to run and select [Offsite Backup Server] to start backing up your files to Quick Backup Server. If applicable, you can change the In-File Delta Type also.



iii. Click [OK] to start backing up your files to Quick Backup Server.

18.4 How to restore Microsoft SQL Server database(s)

Please follow the instructions below to restore your Microsoft SQL Server databases from Quick Backup Server.

Step 1 – Download backup files from Quick Backup Server

1. Download the backup files (.bak) from Quick Backup Server.

   Please refer to the Restoring Files section for information on how to download backup files from Quick Backup Server.

Step 2 – Restore “master" database (Optional)

This step is optional, you need to restore “master" database ONLY if you:

- are rebuilding all your databases from scratch.
- Have changed any server-wide or database configuration options.
- Have added logins or other login security-related operations.
- Have created or removed logical backup devices.
- Have configured the server for distributed queries and remove procedure calls, such as adding linked servers or remote logins.

You do not need to restore your master database if you just want to restore a user database. For more information on Microsoft SQL Server “master" database, please visit http://www.microsoft.com/sql/.

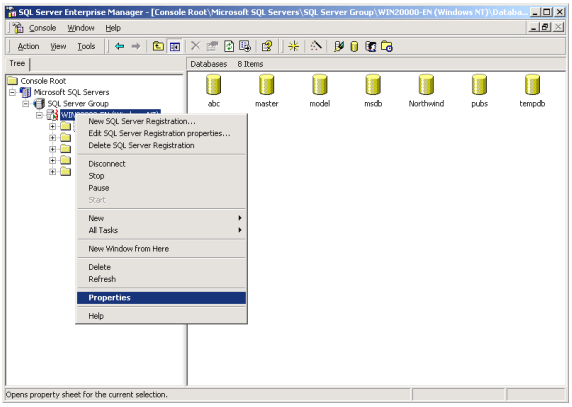
To restore “master" database, please do the following:

1. Open Microsoft SQL Enterprise Manager.

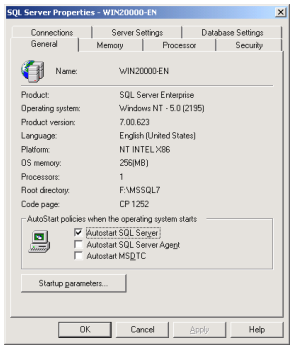
   You can open Microsoft SQL Enterprise Manager from [Start Menu] -> [Program] -> [Microsoft SQL Server] -> [Enterprise Manager]

2. Start Microsoft SQL Server in “Single User Mode".

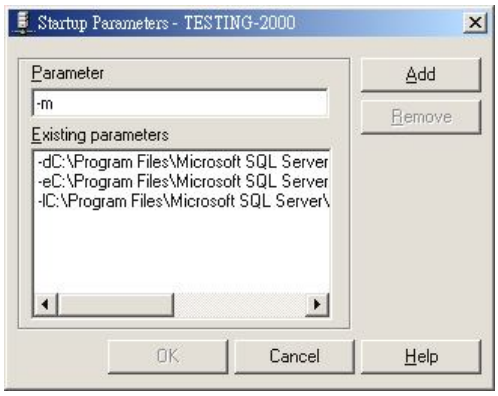
3. Right click your Microsoft SQL Server and select [Properties].



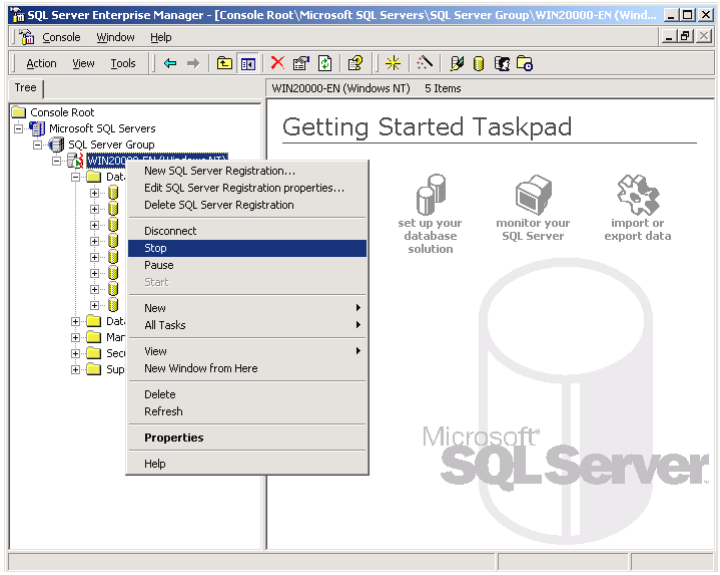
4. Press the [Startup Parameters] button.

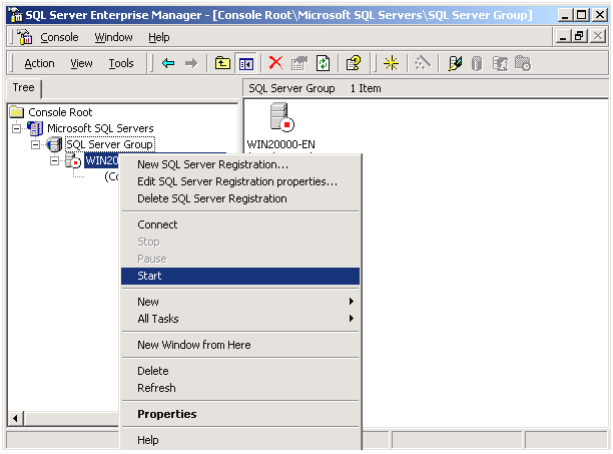


5. Add a “-m" parameter to the [Startup Parameters].



6. Restart Microsoft SQL Server.

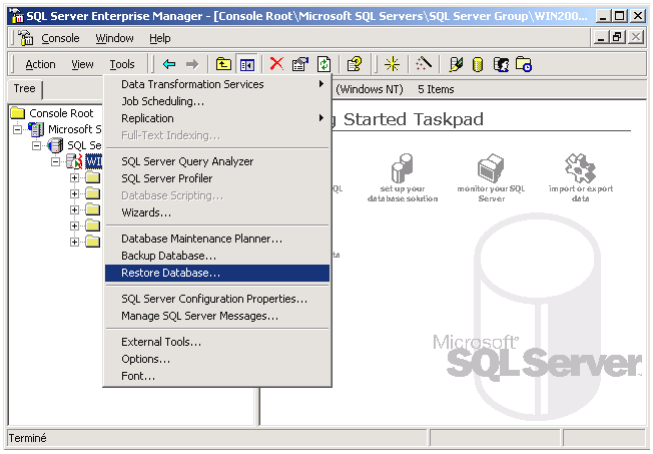




7. From [Enterprise Manager], right click your Microsoft SQL Server and select [Stop] and then [Start.

8. Restore “master" database.

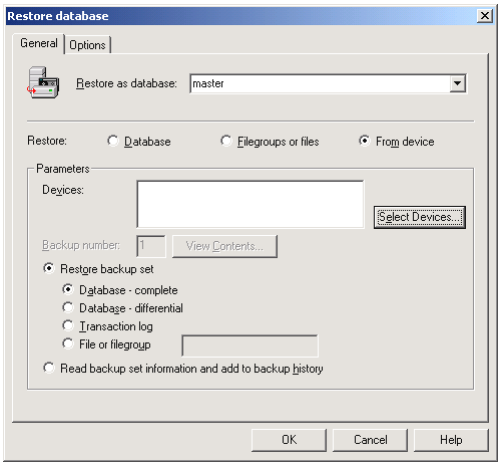
   i. From [Enterprise Manager] -> [Tools] -> [Restore Database].



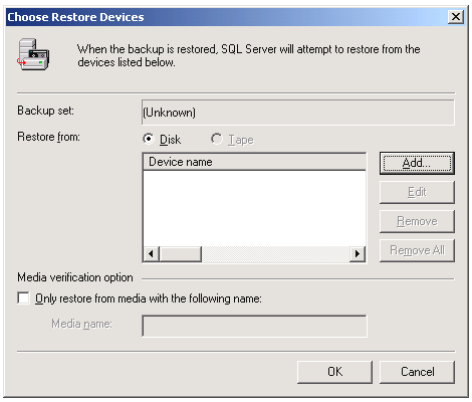
   ii. Select [master] in the [Restore as database] drop down list.

   iii. Select the [from device] radio button.

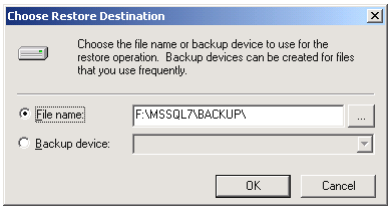
iv. Press the [Select Devices] button.



v. From the [Choose Restore Devices], press the [Add] button.



vi. From the [Choose Restore Destination] panel, press the […] button to choose your master backup (*.bak) from your backup files.


Choose Restore Destination
Choose the file name or backup device to use for the restore operation. Backup devices can be created for files that you use frequently.
File name:
F:\MSSQL7\BACKUP\
Backup device:
OK
Cancel

vii. Press the [OK] button, to start restoring the “master" database.

9. Restart Microsoft SQL Server in “Normal Mode".

i. Remove “-m" parameter from the [Startup Parameters] as in previous step.

ii. Restart your Microsoft SQL Server as in previous step.

Step 3 – Restore “model", “msdb" and distribution" database (Optional)

You need to restore “model" database if you have changed the database template of your SQL Server.

You need to restore “msdb" database if you have changed the scheduling information or you want to restore the backup and restore history of your databases.

You need to restore “distribution" database if you are running the replication components of SQL Server.

You do not need to restore these databases if you just want to restore a user database. For more information on Microsoft SQL Server “model", “msdb" and “distribution" database, please visit http://www.microsoft.com/sql.

You need to restore each of these databases one by one. To restore any of these database, please do the following:

1. From [Enterprise Manager] -> [Tools] -> [Restore Database].

2. Select the database to be restored in the [Restore as database] drop down list.

3. Select the [From device] radio button.

4. Press the [Select Devices] button.

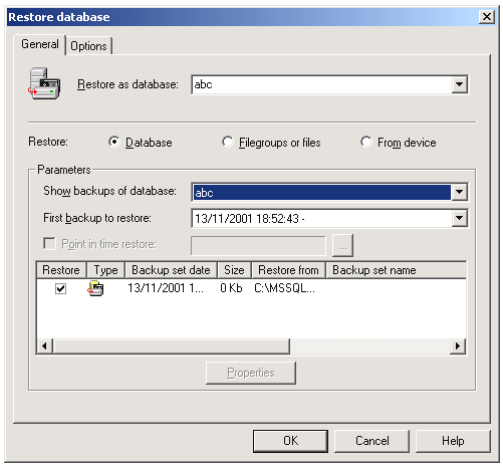
5. Press the […] button to choose your backup files (*.bak) for the database to be restored.

6. Press the [OK] button.

Step 4 – Restore user database(s)

For each of the database you would like to restore,

1. From [Enterprise Manager] -> [Tools] -> [Restore Database].
2. Select the database to be restored in the [Restore as database] drop down list.
3. Select the [Database] radio button.



4. From the [Show backups of database] drop down list, select the database to be restored.
5. From the [First backup to restore] drop down list, select the snapshot of the database you would like to restore to.

   You can restore your database to the snapshot of your database at any point of the time between the time you did your full backup and the time you did your last subsequent backup.

6. Change the [Restore From] Entry.

   If you backup files (*.bak) are not in the default directory, you need to update the full path to your backup files by pressing the [Properties] button.

7. Press the [OK] button.

All database(s) are now restored successfully.

19 Backup/Restore Lotus Domino / Notes

This chapter describes in details on how to use Quick Backup to backup your Lotus Domino Server/ Note Client and how you can restore your Lotus Domino Server / Notes Clients from the backup files.

19.1 Requirements

1. Quick Backup must be installed onto the computer running Lotus Domino Server / Notes Client.

2. Data from Lotus Domino Server / Notes Client will be backed up to a temporary directory before they are sent to Quick Backup Server. Please make sure you have sufficient disk space on your computer to store these data where you run the backup job.

3. Lotus Domino Server must run with archive transaction logging enabled.

   To set up transaction logging in archive style, please do the followings:

   i. Ensure that all databases to be logged reside in the Domino data directory, either at the root or in sub directories.

   ii. From the Domino Administrator, click the Configuration tab.

   iii. In the “Use Directory on" field, choose the server’s Domino Directory.

   iv. Click Server Configuration, and then click Current Server Document.

   v. Click the Transaction Logging tab.

   vi. Complete these fields, and then save the document.

   vii. Restart the computer.

Field	Enter
Transaction Logging	Choose Enabled. The default is Disabled.
Log Path	Path name location of the transaction log. The default path name is \LOGDIR in the Domino data directory, although it is strongly recommended to store the log on a separate, mirrored device, such as a RAID (Redundant Array of Independent Disks) level 0 or 1 device with a dedicated controller. The separate device should have at least 1GB of disk space for the transaction log. If you are using the device solely for storing the transaction log, set the [Use all available space on log device] field to “Yes"
Logging Style	Choose [Archive]. The default is [Circular].
Maximum Log Space	The maximum size in MB, for the transaction log. Default is 192MB. Maximum is 4096MB (4GB). Domino formats at least 3 and up to 64 log files, depending on the maximum

	log space you allocate.
Use all available space on log device	Choose one: - [Yes] to use all available space on the device for the transaction log. This is recommended if you use a separate device dedicated for storing the log. If you choose [Yes], you do not need to enter a value in the [Maximum Log Space] field. - [No] to use the default or specified value in the [Maximum Log Space] field.
Automatic fixup of corrupt databases	Choose one: - Enabled (default). If a database is corrupted and Domain cannot use the transaction log to recover it, Domino runs the Fixup task, assigned a new DBIID, and notifies the administrator that a new database backup is required. - Disabled. Domino does not run the Fixup task automatically and notifies the administrator to run the Fixup task with the –J parameter on corrupt logged databases.
Runtime / Restart performance	This field controls how often Domino records a recovery checkpoint in the transaction log, which affects server performance. To record a recovery checkpoint, Domino evaluates each active logged database to determine how many transactions would be necessary to recover each database after a system failure. When Domino completes this evaluation, it: - Creates a recovery checkpoint record in the transaction log, listing each open database and the starting point transaction needed for recovery. - Force database changes to be saved to disk if they have not been saved already Choose one: - Standard (default and recommended). Checkpoints occur regularly. - Favor runtime. Domino records fewer checkpoints, which requires fewer system resources and improves server run time performance. - Favor restart recovery time. Domino records more checkpoints, which improves restart recovery time because fewer transactions are required for recovery.

Notes:

You can only run transaction log backup if you have transaction logging enabled and you are using archive mode. This command does not apply if you have transaction logging enabled not in archive mode or if transaction logging is not enabled at all. If you try to issue it, you will receive an error message.

19.2 Overview

Quick Backup will backup your Lotus Domino Server / Notes Client by taking the following steps:

1. Run all Pre-Commands of this backup set.
2. If the backup type to run is [Database Backup Type],
   i. All file(s) / database(s) selected are copied to the temporary directory specified by this backup set.
   ii. The notes.ini file, if selected, will be copied to the temporary directory.
   iii. Only filled log extents will be copied to the temporary directory, and the Domino server is notified of their availability for reuse (for Domino server only).
3. (For Domino Server Only) If the backup type to run is [Transaction Log Backup Type],
   i. Only filled log extents will be copied to the temporary directory, and the Domino Server is notified of their availability for reuse.
4. Run all Post-Commands of this backup set.
5. Upload all files copied to the temporary to Quick Backup Server.
6. Remove temporary files from the temporary directory.

19.3 How to backup Lotus Domino / Notes on Windows

Please follow the instructions below to backup the database(s)/file(s) of your Lotus Domino Server /Notes Clients using Quick Backup.

1. Open Quick Backup.

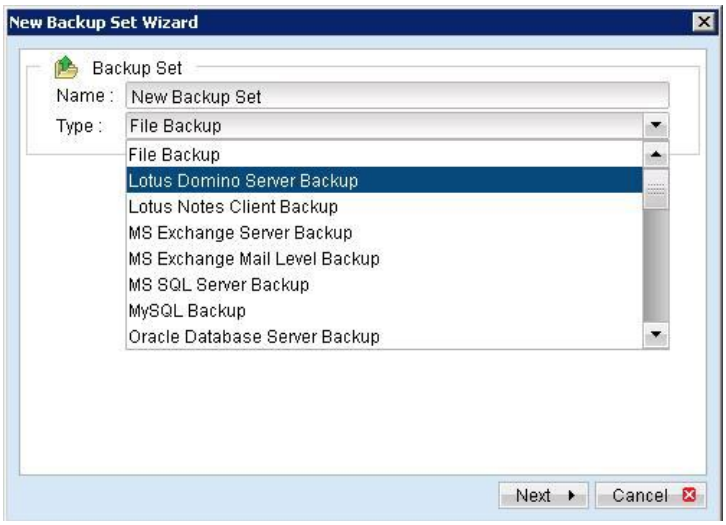
   Right click Quick Backup icon available in the system tray and choose [Open].

2. Create a backup set.

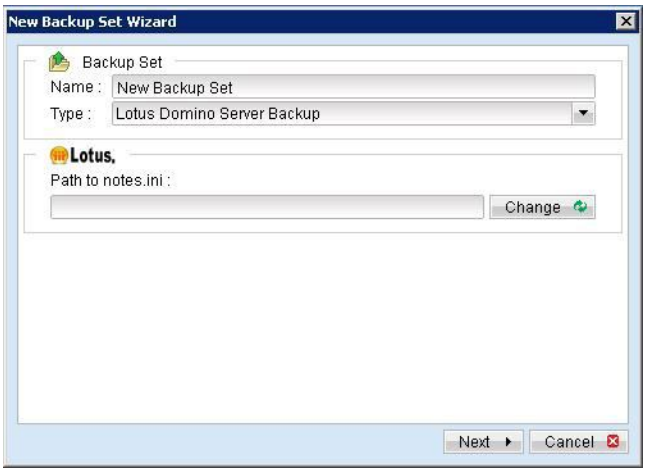
i. To start setting up backup sets, click the button to open the [Backup Setting] dialog.

ii. On the left panel, press the button to create a new backup set.

iii. On the dialog, choose [Lotus Domino Server Backup] (or [Lotus Notes Client Backup] for Lotus Notes) as the [Type].



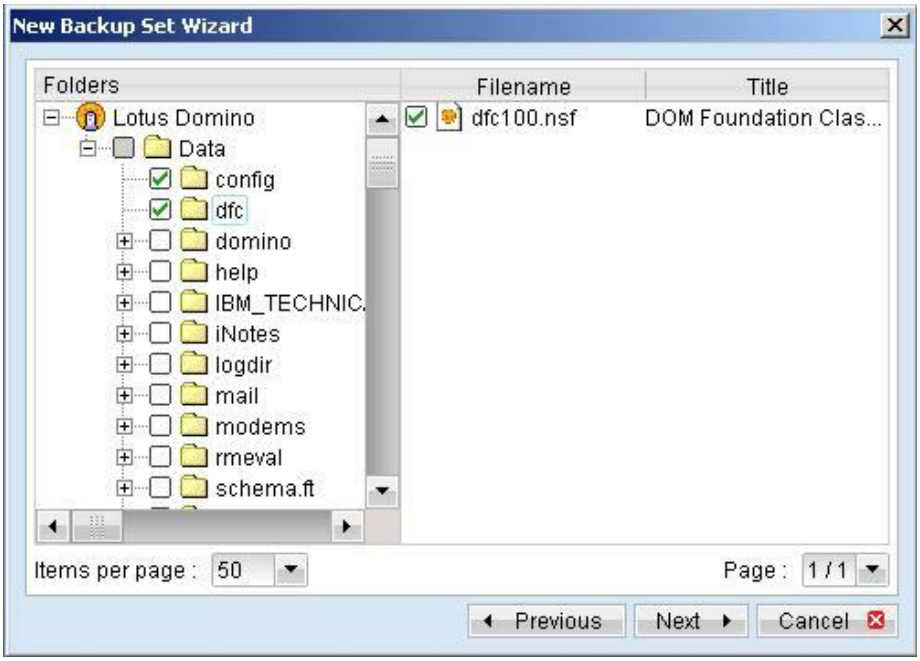
iv. Enter a name for your backup set.



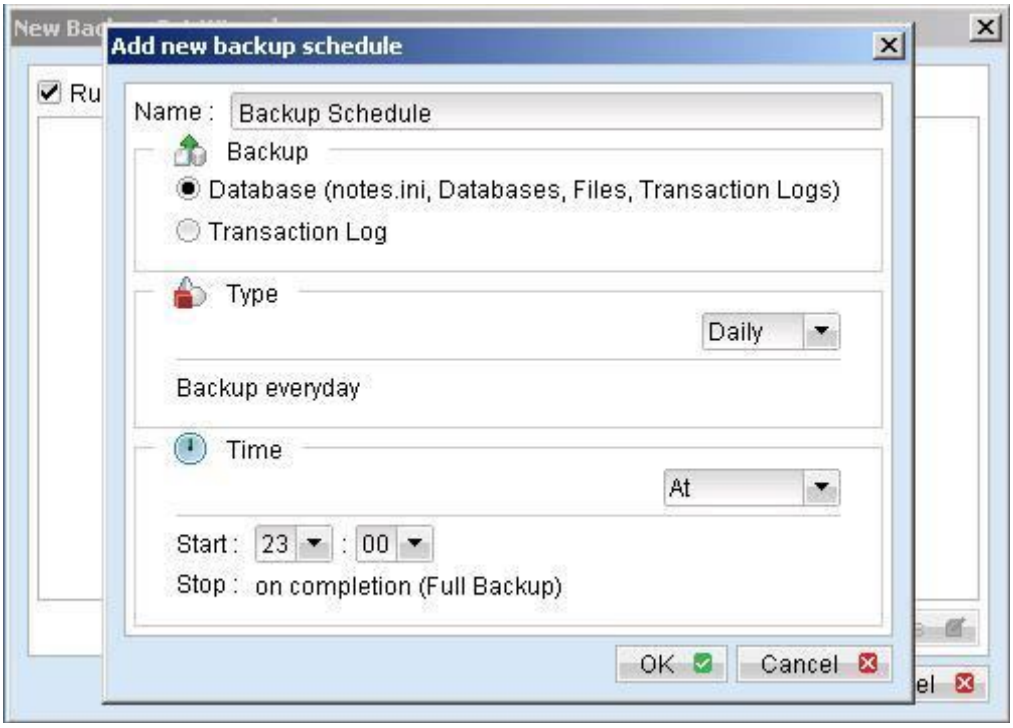
v. Select the location of the “note.ini" file.

vi. Select the database(s) / file(s) you want to backup.

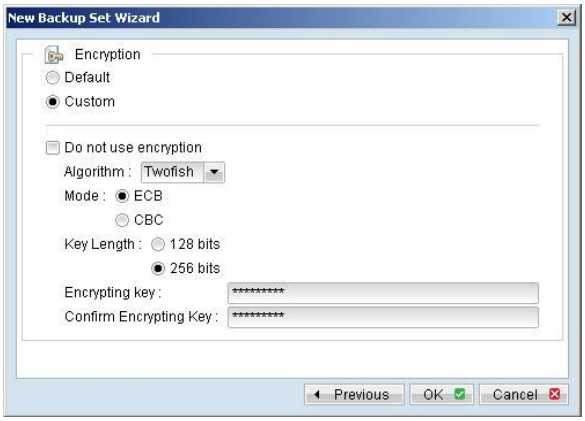
vii. Set the backup schedule for Database Backup.



viii. Set the backup schedule for Transaction Log Backup (for Domino server only). (Note: You can have more than one schedule in a backup set, i.e. you can perform intra-day transaction log backup by adding more than one daily transaction log backup schedule to your backup set).



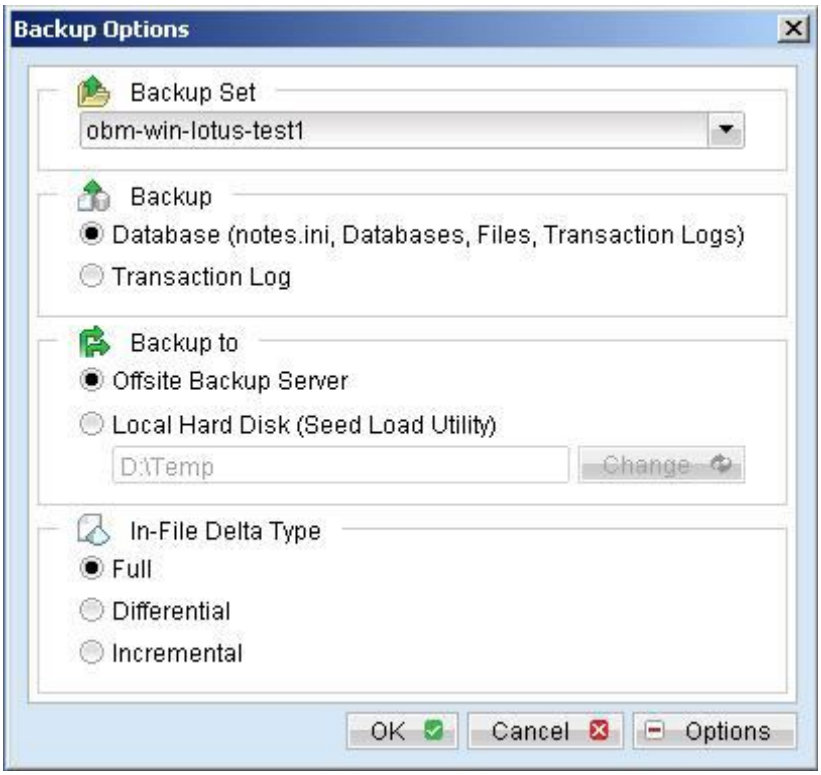
ix. Set the encryption algorithm, encryption mode and encrypting key for this backup set. (Hint: For maximum security, please select AES (Advanced Encryption Standard) Algorithm, CBC (Cipher Block Chaining) mode and use an encrypting key with more than 8 characters).



3. Run Backup

i. Press the [Backup] button on the main page of Quick Backup dialog.

ii. Select the backup type (e.g. Database, Transaction Log) you would like to perform (for Domino server only). Select the backupset you want to run and select [offsite Backup Server] to start backing up your files to Quick Backup Server. If applicable, you can change the In-File Delta Type also.



iii. Click [OK] to start backing up your files to Quick Backup Server.

19.4 How to restore Lotus Domino / Notes on Windows

Please follow the instructions below to restore the database(s)/file(s) of Lotus Domino Server / Notes Client from Quick Backup Server.

1. Install Lotus Domino Server / Notes Client back to its original folder (if required).

2. Install Quick Backup.

   Please refer to the Installing Quick Backup section for information on how to install Quick Backup onto your computer.

3. Shutdown Lotus Domino Server.

Restore All Databases and files

If you want to perform a full domino restore (restore all databases and files):

1. Download the backup files to be restored from Quick Backup Server and save them back to its original location. It includes “notes.ini", all backup files from the lotus domino data directory and all archived transaction logs.

2. Modify the “DominoRecover.bat" located under the bin directory of Quick Backup installation to reflect your setup. You need to specify the Lotus executable directory.

   For example change the PROGRAM_DIR to:

```
PROGRAM_DIR=C:\Lotus\Domino
```

3. Run “DominoRecover.bat" and press ‘Y’ to continue.

   For example:

```
C:\Program Files\obm\bin\DominoRecover.bat
```

   This will run media recovery for all database (*.nsf and mail.box) found under the Lotus data directory (e.g. C:\Lotus\Domino\Data). You should see something similar to the screen below.

Media Recovery Example:

```
C:\program files\obm\bin>DominoRecover.bat
Media Recovery Utility for Lotus Domino 5.0 or above

Please make sure that you have done the following:
1. Reinstall Lotus Domino on this computer in the same directory
2. Restore Notes.ini to the Lotus Domino installation directory
   (e.g. C:\Lotus\Domino)
3. Restore Domino Data directory back to the directory defined
   in Notes.ini (e.g. C:\Lotus\Domino\Data)
4. Restore all archived transaction logs to the directory defined
   in Notes.ini (e.g. C:\Lotus\Domino\Data\logdir)
```

Continue ? (Y) or (N) y
Running media recovery ...
Please wait, creating new transaction logs in directory: C:\logdir
02/12/2003 14:39:19 Recovery Manager: Restart Recovery complete. (0/0 databases needed full/partial recovery)
Media Recovery Replay (122 MB): 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
02/12/2003 14:39:22 Recovery Manager: Media Recovery complete for C:\Lotus\Domino\Data\admin4.nsf, last update applied .

Backup file C:\Lotus\Domino\Data\admin4.nsf recovered.

……

Media Recovery Replay (122 MB): 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%
02/12/2003 14:40:57 Recovery Manager: Media Recovery complete for C:\Lotus\Domino\Data\statrep.nsf, last update applied .

Backup file C:\Lotus\Domino\Data\statrep.nsf recovered.

C:\program files\obm\bin>

4. All content of all database(s) are now rolled forward to the last committed transaction found in the last archived transaction log.

5. Restart Lotus Domino Server.

Restore a single database

If you just want to restore a single database:

1. Download the database file to be restored from Quick Backup Server and save them back to its original location.

2. (Optional) If you need to perform media recovery on this database, please download all archived transaction logs and save them back to its original location.

3. Modify the “DominoRecover.bat" located under the bin directory of the Quick Backup installation to reflect your setup.

   For example we will recover the “admin4.nsf" and have restored the file to C:\restore\notesdata, change the tags to:

```
PROGRAM_DIR=C:\Lotus\Domino
INPUTFILE=C:\restore\notesdata\admin4.nsf
RESTOREDB=C:\Lotus\Domino\Data\admin4.nsf
RECDATE=18/01/2007
RECTIME=00:02
```

4. Run “DominoRecover.bat".

   You should see something similar to the screen below.

Media Recovery Example:

```
C:\program files\obm>DominoRecover.bat
Media Recovery Utility for Lotus Domino 5.0 or above

Running media recovery ...
Restart Analysis (0 MB): 100%
18/01/2007 14:42:15   Recovery Manager: Restart Recovery complete. (0/0
databases needed full/partial recovery)
Media Recovery Replay (122 MB): 10% 20% 30% 40% 50% 60% 70% 80% 90%
100%
18/01/2007 14:42:17   Recovery Manager: Media Recovery complete for
C:\Lotus\Domino\data\admin4.nsf, last update applied .

 Backup file C:\Lotus\Domino\data\admin4.nsf recovered.


C:\Lotus\Domino>
```

5. All content of the database are now rolled forward to the last committed transaction found in the last archived transaction log.

6. Restart Lotus Domino Server.

19.5 How to backup Lotus Domino / Notes on Linux

Before setting up Quick Backup, please make sure that the user running Quick Backup have sufficient privileges to read and write to the “notesenv" file located in the bin subdirectory of where Quick Backup is installed. This file is used by Quick Backup to

store the location of the Domino/Notes application executables. E.g. use chmod to set read, write & execute permissions:

```
# cd $Quick Backup_HOME/bin
# chmod 777 notesenv
```

Please follow the instructions below to backup the database(s)/file(s) of your Lotus Domino Server / Notes Client using Quick Backup:

1. Open Quick Backup by typing the following in a terminal.

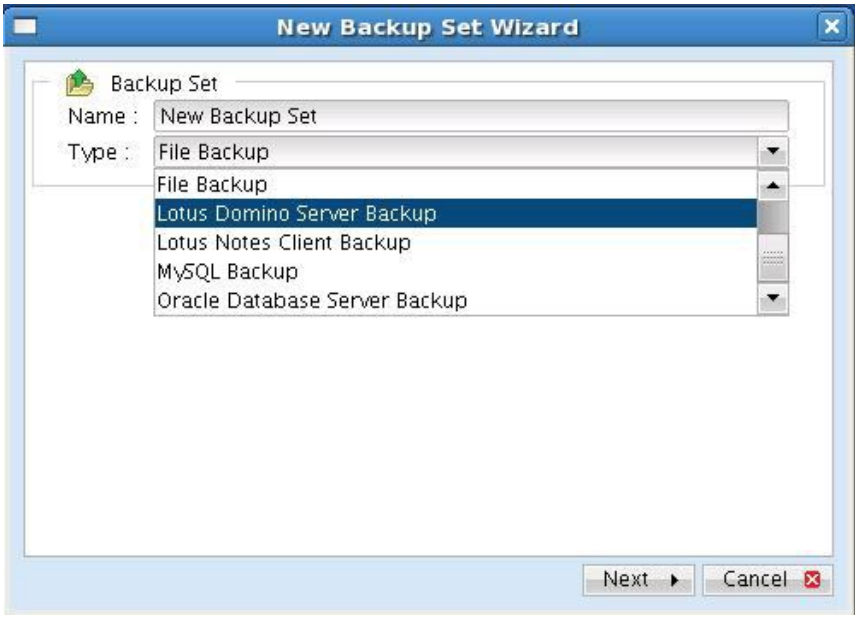
```
# cd $Quick Backup_HOME
# ./bin/RunOBC.sh
```

2. Create a backup set.

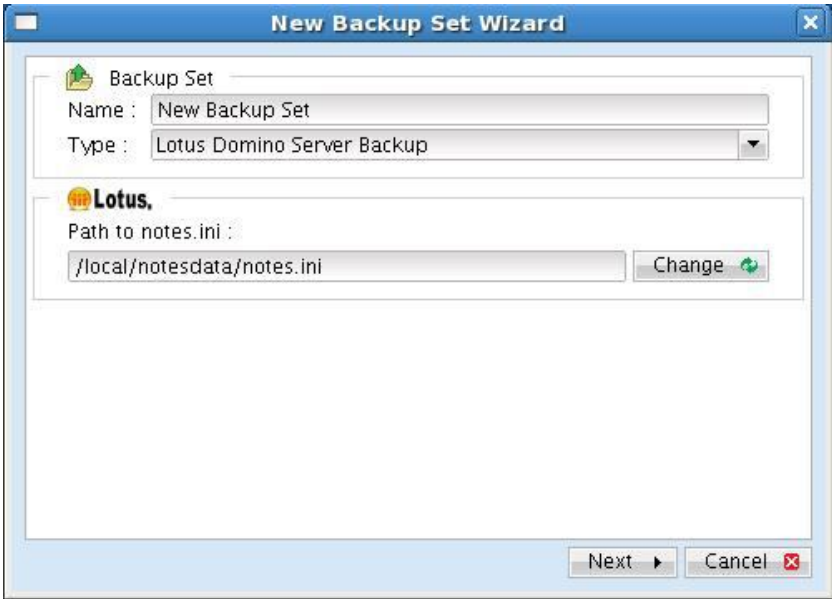
   i. To start setting up backup sets, click the button to open the [Backup Setting] dialog.

   ii. On the left panel, press the button to create a new backup set.

   iii. On the dialog, choose [Lotus Domino Server Backup] (OR [Lotus Notes Client Backup] for Lotus Notes) as the [Type].



   iv. Enter a name for your backup set.

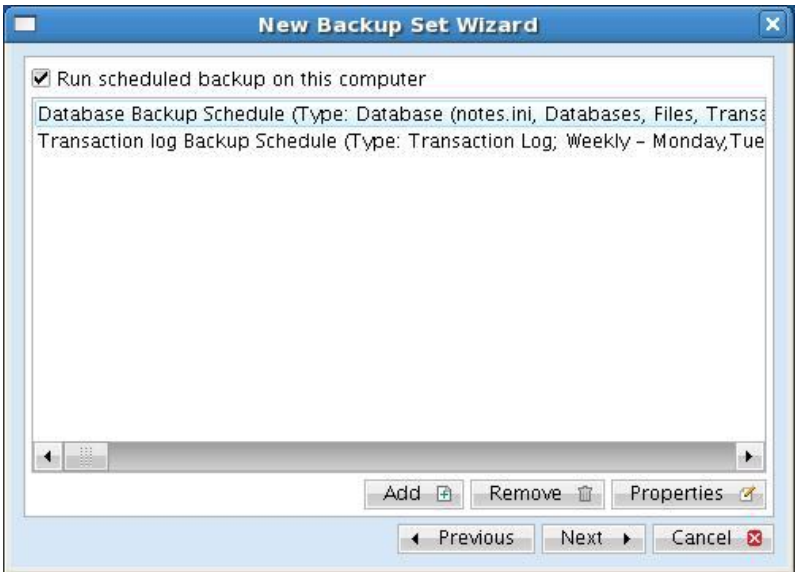


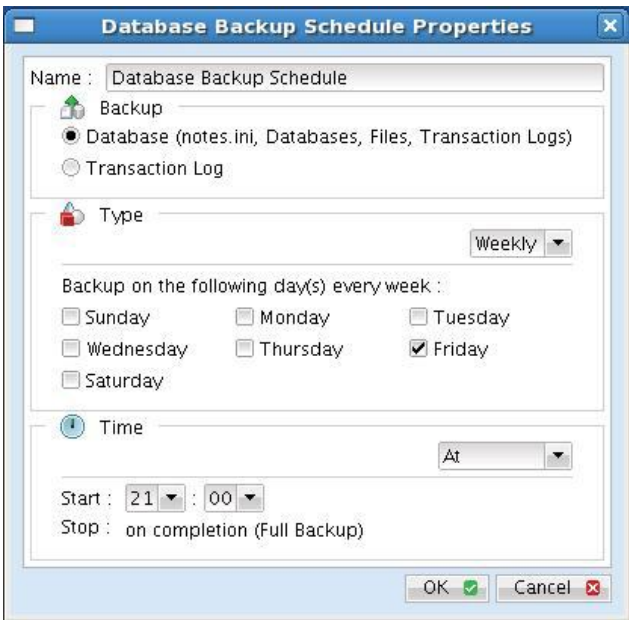
v. Select the location of the “note.ini" file. The default path for this will be in the /local/notesdata folder.

vi. Select the database(s) / file(s) you want to backup.

vii. Enter a temporary location to store the backup files before they are sent to Quick Backup Server. Please make sure that the user running Quick Backup have sufficient privileges to read and write to this location and sufficient space is available.

viii. Set the backup schedule for Database Backup.





ix. Set the backup schedule for Transaction Log Backup (for Domino server only). (Note: You can have more than one schedule in a backup set, i.e. you can perform intra-day transaction log backup by adding more than one daily transaction log backup schedule to your backup set).

x. Set the encryption algorithm, encryption mode and encrypting key for this backup set.

New Backup Set Wizard
Encryption
Default
Custom
Do not use encryption
Algorithm :
Twofish
Mode :
ECB
CBC
Key Length :
128 bits
256 bits
Encrypting key :
Confirm Encrypting Key :
Previous
OK
Cancel

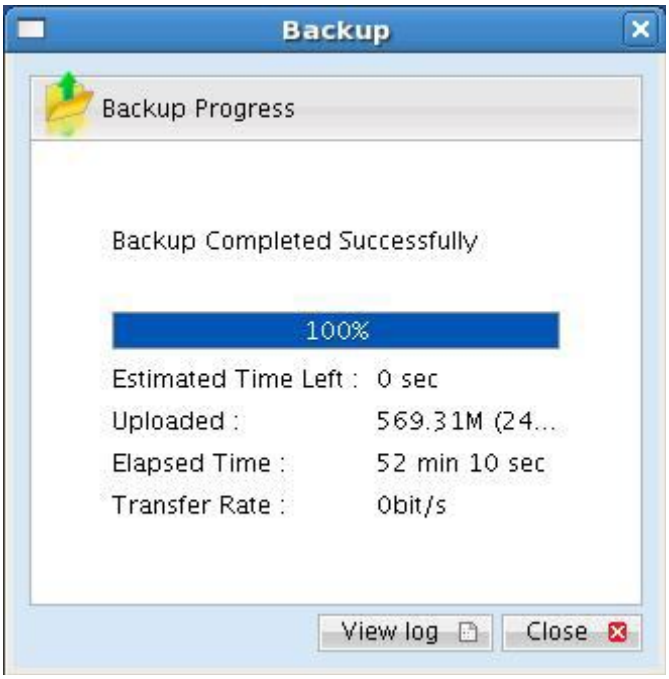
3. Run Backup.

i. Press the [Backup] button on the main page of Quick Backup dialog.

ii. Select the backup type (e.g. Database, Transaction Log) you would like to perform (for Domino server only). Select the backup set you want to run and select [Offsite Backup Server] to start backing up your files to Quick Backup Server. If applicable, you can change the In-File Delta Type also.

iii. Click [OK] to start backing up your files to Quick Backup Server.

iv. You should get something similar to the screen shot below.



19.6 How to restore Lotus Domino / Notes on Linux

Please follow the instructions below to restore database(s) / file(s) of your Lotus Domino Server/ Notes client from Quick Backup Server.

Preparations

1. Install Lotus Domino Server / Notes client back to its original folder (if required).

2. Install Quick Backup.

   Please refer to the Installing Quick Backup section for information on how to install Quick Backup onto your computer.

3. Shutdown Lotus Domino Server.

Restore a full Domino Server

Please follow the instructions to perform a full Domain restore (restore all databases and files).

1. Download the backup files to be restored from Quick Backup Server and save them back to its original location. It includes notes.ini, all backup files from the lotus domino data directory and all archived transaction logs. If you encounter any access problems, please try restoring using the “root" user.

2. Make sure that the owner and group permissions of the restored files are the notes user.

   For example:

```
# chown –R notes:notes /local/notesdata
```

   This will assign the owner and group to all files and directories within /local/notesdata.

3. Modify the “DominoRecover.sh" located under the bin directory of the Quick Backup installation to reflect your setup. You need to specify the data directory and the lotus executable directory.

   For example change the DATA_DIR and LOTUS tags to:

```
DATA_DIR=/local/notesdata
LOTUS=/opt/ibm/lotus
```

4. Make sure the current user is the notes user before running the “DominoRecover.sh"

5. Run “DominoRecover.sh" and press [Y] to continue.

   For example:

```
#./usr/local/obm/bin/DominoRecover.sh
```

This will run media recovery for all databases (*.nsf and mai.box) found under the Lotus data directory (e.g. /local/notesdata). You should see something similar to the screen below.

Media Recovery Example:

bash-3.00$ cd /usr/local/obm/bin
bash-3.00$ ./DominoRecover.sh
Media Recovery Utility for Lotus Domino 5.0 or above

Please make sure that you have done the following:
1. Reinstall Lotus Domino on this computer in the same directory
2. Restore Notes.ini to the Lotus Domino installation directory
(e.g. /local/notesdata)
3. Restore Domino Data directory back to the directory defined
in Notes.ini (e.g. /local/notesdata)
4. Restore all archived transaction logs to the directory defined
in Notes.ini (e.g. /local/notesdata/logdir)

Continue ? (Y) or (N) y

Running media recovery ...
directory /local/notesdata// already exists
Please wait, creating new transaction logs in directory: /local/notesdata/logdir/
02/01/2007 11:38:43 AM Recovery Manager: Restart Recovery complete. (0/0 databases needed full/partial recovery)
02/01/2007 11:38:45 AM Recovery Manager: Assigning new DBIID for /local/notesdata/names.nsf (need new backup for media recovery).
Media Recovery Replay (0 MB): 100%
02/01/2007 11:38:45 AM Recovery Manager: Media Recovery complete for /local/notesdata/dfc/dfc100.nsf, last update applied .

Backup file /local/notesdata/dfc/dfc100.nsf recovered.
Media Recovery Replay (0 MB): 100%
02/01/2007 11:38:46 AM Recovery Manager: Media Recovery complete for /local/notesdata/help/decsdoc.nsf, last update applied .

…

Backup file /local/notesdata/iNotes/help70_iwa_en.nsf recovered.
Media Recovery Replay (0 MB): 100%
02/01/2007 11:38:50 AM Recovery Manager: Media Recovery complete for /local/notesdata/mail/notes.nsf, last update applied .

Backup file /local/notesdata/mail/notes.nsf recovered.
bash-3.00$

6. All content of all database(s) are now rolled forward to the last committed transaction found in the last archived transaction log.

7. Restart Lotus Domino Server.

Restore Single Database

Please follow the instructions to restore a single database:

1. Download the database file to be restored from Quick Backup Server and save them back to its original location.

2. (Optional) If you need to perform media recovery on this database, please download all archived transaction logs and save them back to its original location.

3. Modify the “DominoRecover.sh" located under the bin directory Quick Backup installation to reflect your setup.

   For example, we will recover the “admin4.nsf" and have restored the file to /restore/local/notesdata, change the tags to:

```
DATA_DIR=/local/notesdata
LOTUS=/opt/ibm/lotus
        INPUTFILE=/restore/local/notesdata/admin4.nsf
RESTOREDB=/local/notesdata/admin4.nsf
RECDATE=18/01/2007
RECTIME=22:41
```

4. Make sure the current user is the notes user before running the “DominoRecover.sh".

5. Run “DominoRecover.sh".

   You should see something similar to the screen below.

Media Recovery Example:

```
bash-3.00$ cd /usr/local/obm/bin
bash-3.00$ ./DominoRecover.sh
Media Recovery Utility for Lotus Domino 5.0 or above

directory /local/notesdata// already exists

 Recovering backup file ...

Restart Analysis (0 MB): 100%
18/01/2007 03:35:56 PM  Recovery Manager: Restart Recovery complete. (0/0
databa ses needed full/partial recovery)
Media Recovery Replay (1 MB): 30% 50% 80% 100%
18/01/2007 03:35:57 PM  Recovery Manager: Media Recovery complete for
/local/res tore/local/notesdata/admin4.nsf, last update applied .

 Backup file /local/restore/local/notesdata/admin4.nsf recovered.

 Taking database /local/notesdata/admin4.nsf offline ...


 Restoring database /local/notesdata/admin4.nsf
  from recovered backup file /local/restore/local/notesdata/admin4.nsf ...
Database file /local/notesdata/admin4.nsf restored from /local/restore/local/not
esdata/admin4.nsf

 Bringing database /local/notesdata/admin4.nsf online ...
```

```
Program completed successfully.
bash-3.00$
```

6. All content of the database are now rolled forward to the last committed transaction found in the last archived transaction log.

7. Restart Lotus Domino Server.

20 Backup/Restore MySQL Server

This chapter describes in details how to use Quick Backup to backup/restore your MySQL Server and how you can restore your MySQL server from the database backup files.

20.1 Requirements

Please make sure the following requirements are met before you can backup MySQL using Quick Backup.

1. Quick Backup must be installed on the computer running MySQL server.
2. Data from MySQL server will be backed up to a temporary directory before they are sent to Quick Backup Server. Please make sure you have sufficient space on your computer to store these data when you run the backup job.
3. There must be a MySQL account that can be used to connect from localhost. For example:

```
mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'localhost' IDENTIFIED BY
  'some_pass';
mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'localhost.localdomain' IDENTIFIED
  BY 'some_pass';
mysql> FLUSH PRIVILEGES;
```

They are superuser accounts with full privileges to do anything with a password of some_pass.

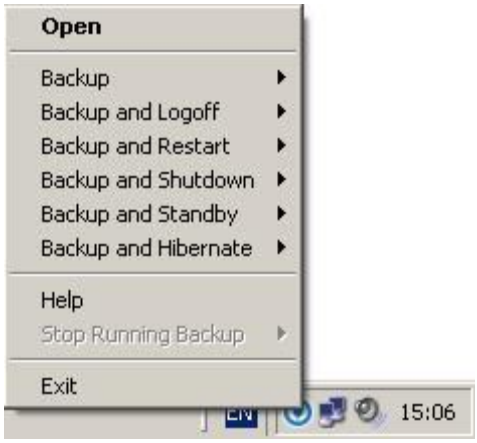
20.2 Overview

Quick Backup will backup your MySQL server by taking the following steps:

1. Run all Pre-Commands of this backup set.
2. All database(s) (either local or external) selected are backed up to a temporary directory specified in its backup set.
3. Run all Post-Commands of this backup set.
4. Upload all backup files from the temporary directory to Quick Backup Server.
5. Remove temporary files from the temporary directory if [Setting] -> [Remove Temporary files after backup] is enabled.

20.3 How to backup MySQL server on Windows

1. Open Quick Backup and right click Quick Backup icon available in the system tray and choose [Open].

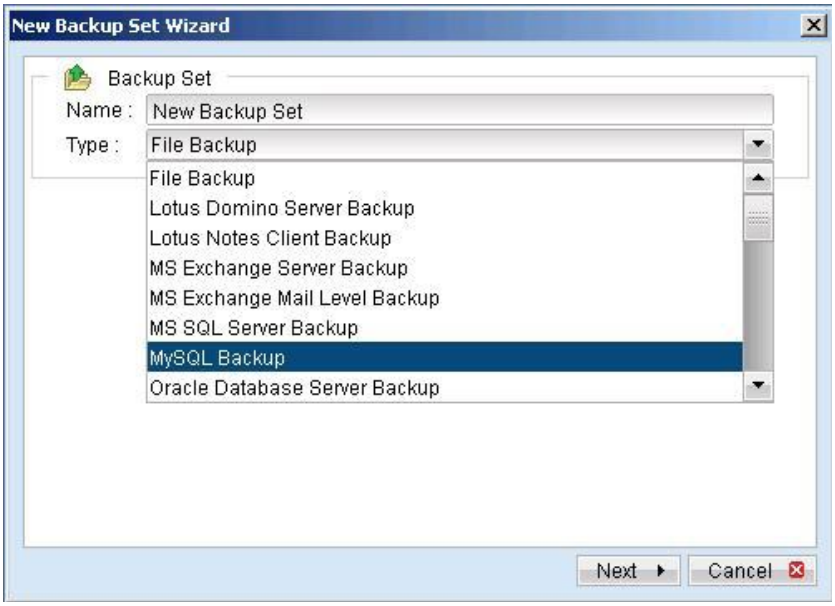


2. From the Menu, Choose [Backup Set] -> [New] -> [MySQL Backup Set] to create a backup set:

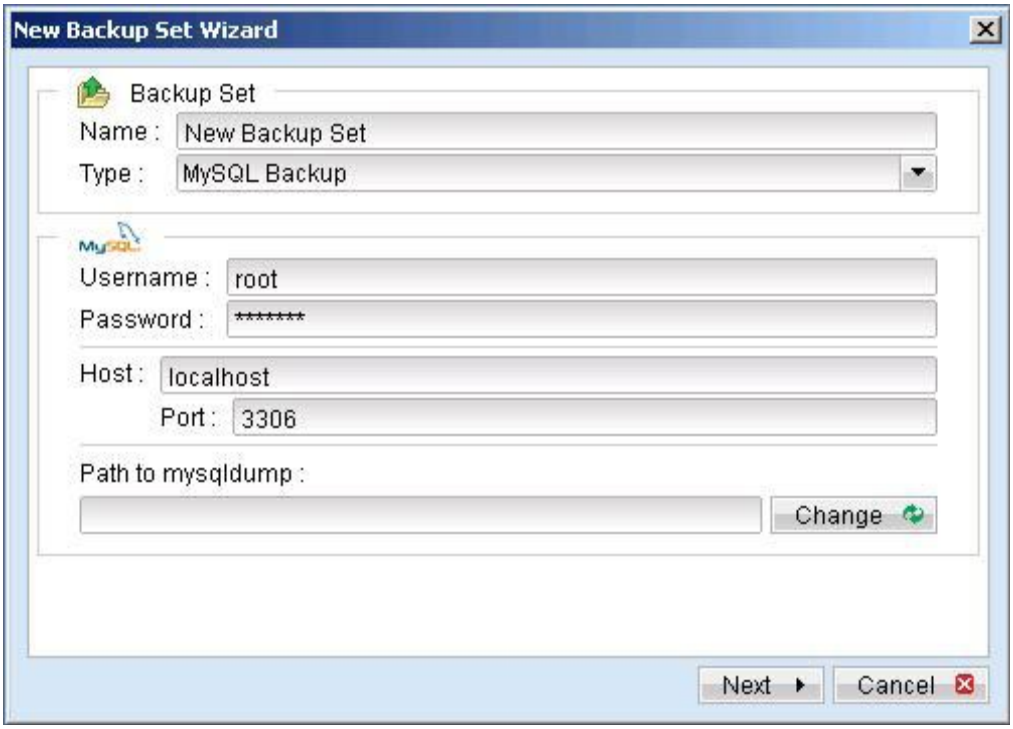
   i. To start setting up backup sets, click the button to open the [Backup Setting] dialog.

   ii. On the left panel, press the button to create a new backup set.

   iii. On the dialog, choose [MySQL Backup] as the [Type].

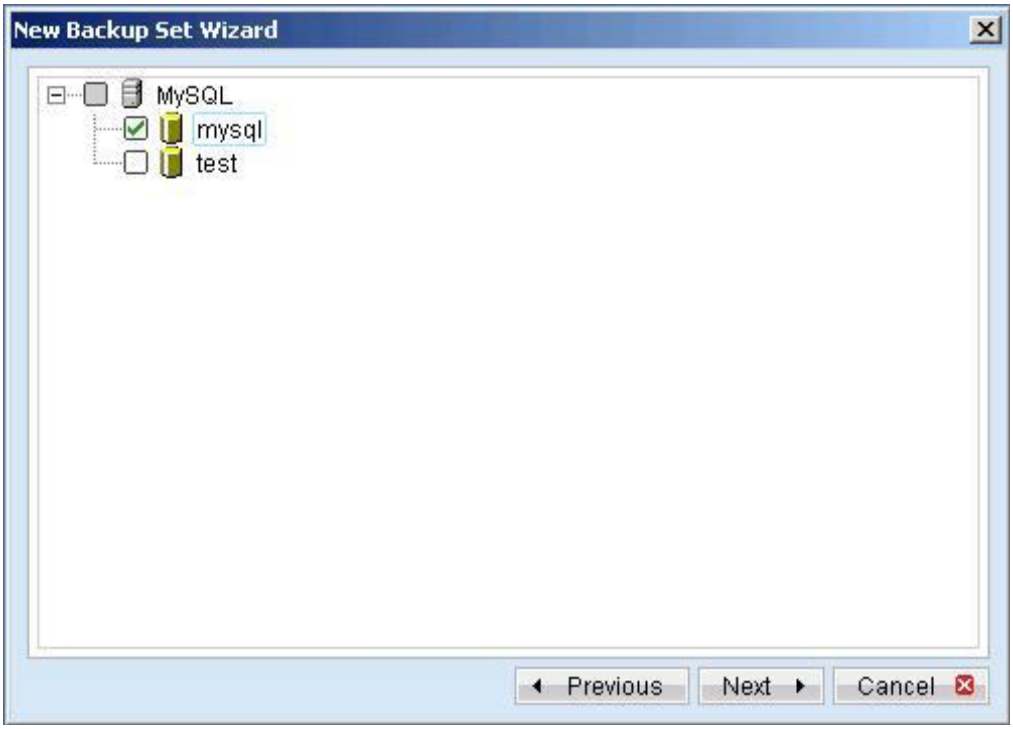


   iv. Enter name for your backup set.



v. Enter the root password, the MySQL server TCP/IP port number and the path to MySQL backup utility (mysqldump).

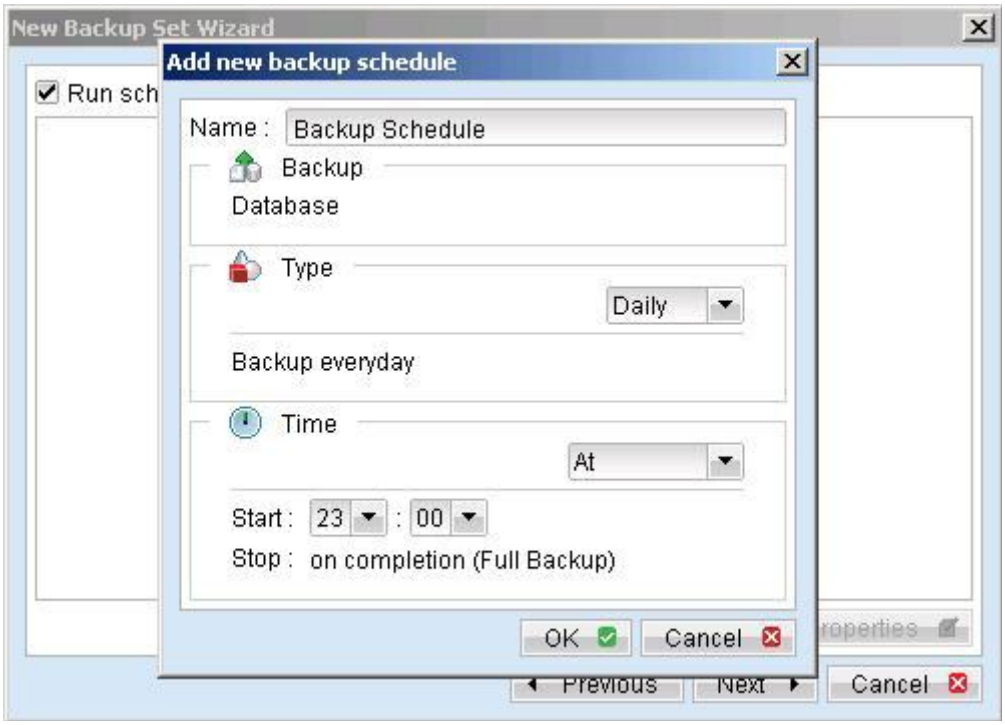
vi. Select the database(s) to be backed up.



vii. Enter a temporary directory for storing the backup files before they are sent to Quick Backup Server,

e.g. C:\Backup\MySQL

viii. Set the backup schedule for Database Backup.



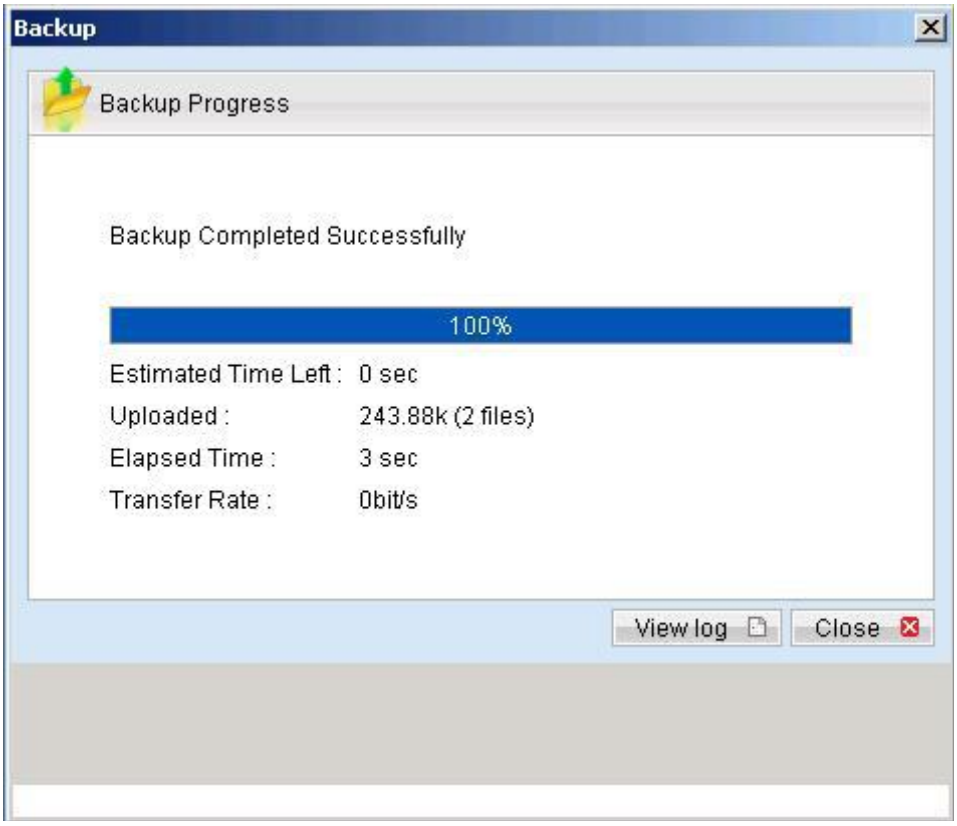
ix. Set the encryption algorithm, encryption mode and encrypting key for this backup set.

3. Run Backup

i. Press the [Backup] button on the main page of Quick Backup dialog.

ii. Select the backup set you want to run and select [Offsite Backup Server] to start backing up your files to Quick Backup Server. If applicable, you can change the In-File Delta Type also.

iii. You should get something similar to the screen shot below.



20.4 How to backup MySQL server on Linux (command line mode)

If you want to setup Quick Backup to backup MySQL Server running on Linux using command line mode, please do the followings:

1. Create a backup account on Quick Backup Server.

2. Logon to the web interface of Quick Backup Server using the backup account created in the previous step. (It does not matter if it is not from the Linux server running the MySQL server to be backed up).

3. Create a new backup set by pressing the [Backup Set] -> [Add] button.

4. Select the [Backup Set] -> [Type] -> [MySQL Database Server] radio button and press [Update] button (which can be found at the bottom of the page).

5. Setup all [Backup Set] -> [Database Backup Setting].

Settings	Descriptions
MySQL Username (e.g. root)	**A MySQL user account that has backup access to the database to be backed up (e.g. root). Please refer to the requirements section for information.**
MySQL Password	**Password of the MySQL user account being used.**
Hostname	**IP address/Hostname of the MySQL Server, e.g.**
MySQL Connection TCP/IP Port	**TCP/IP port used to access the MySQL Server (default: 3306)**
Path to MySQL backup utility (mysqldump)	**Full path to where mysqldump can be found (e.g. /usr/bin/mysqldump)**
Temporary Directory	**A temporary directory to be used to store all MySQL database dump files before they are uploaded to the backup server.**
Enable Delete Temp. File	**Whether to delete the temporary MySQL database dump files after they are uploaded to the backup server.**

6. Setup the [Backup Set] -> [Backup Source] setting.

   - Add a “MySQL" entry to the [Backup Source] if you want to backup all databases under this MySQL server.
   - Add two entries, “MySQL/database1" and “MySQL/database2", to the [Backup Source] if you want to backup both “database1" and “database2" under this MySQL Server.

   (Please use “\" instead of “/" if the MySQL Server to be backed up is running on Windows instead of Linux).

7. Setup the [Backup Set] -> [Backup Schedule] by pressing the [Add] link next to the “Backup Schedule" sub-title.

8. Install Quick Backup onto the Linux Server (Please refer to Section 3 for details. The command line mode installation instructions are available on the web interface).

9. Configure RunBackup.sh to perform the backup of MySQL Server.

   If you have started up the Quick Backup backup scheduler in the previous step, selected databases will be backed up automatically at scheduled time.

20.5 How to restore MySQL server

Please follow the instructions below to restore MySQL server from Quick Backup Server.

1. Download the database backup files to be restored from Quick Backup Server.

   Please refer to Restoring Files Section for information on how to download backup files from Quick Backup Server.

2. Restore the database named [db_name] from the database backup file [db_name.sql]:

   i. Connect to the MySQL Server.

   ```
   (Windows) C:\>mysql
   (Linux)[root@server ~]# mysql
   ```

   ii. Create the database to be restored.

   ```
   mysql> CREATE DATABASE IF NOT EXISTS db_name
   ```

   iii. Restore the database backup file back into the MySQL server.

   ```
   mysql> use db_name;
   mysql> source db_name.sql;
   ```

   If db_name.sql is not located in the current directory, please specify the full path to the db_name.sql file in the command above.

3. Repeat the same procedure for each database to be restored to the MySQL Server.

4. The MySQL Server is restored successfully.

21 Email Reporting

Quick Backup Server makes use of the email system to keep you informed with the status of your backup activities. Please make sure your contact information within the backup system is correct to receive the reports described in this chapter.

21.1 New User Report

When a new backup account is added to the backup server, a new user report will be delivered to the contact email(s) of the new account. The New User Report contains the following information:

Sample Report

Online Backup
Generated at: Tue Aug 12 18:07:04 CST 20
Getting started:
Please follow the instructions available in the installation wizard to download and install AhsayOBM.
Further Information:
If further assistance is required, please refer to the FAQs.
User Setting
Login Name :NewAccount
Alias :NewAccount Name
Language :English
Contact :new_account@your-company.com
Backup Quota :50M

Key	Description
Login Name	Login Name
Alias	Alias
Language	Preferred Language for your backup report.
Contact	Email Address that will be used to contact you.
Backup Quota	Backup quota

21.2 Forgot Password Report

If you have forgotten your password, you can use the [Forgot Password] feature available on the web interface to have your password delivered to you through email. (Please refer to “Retrieve Forgotten Password" section in the next chapter for more information on how to retrieve your forgot password report.) The Forgot Password Report contains the following information:

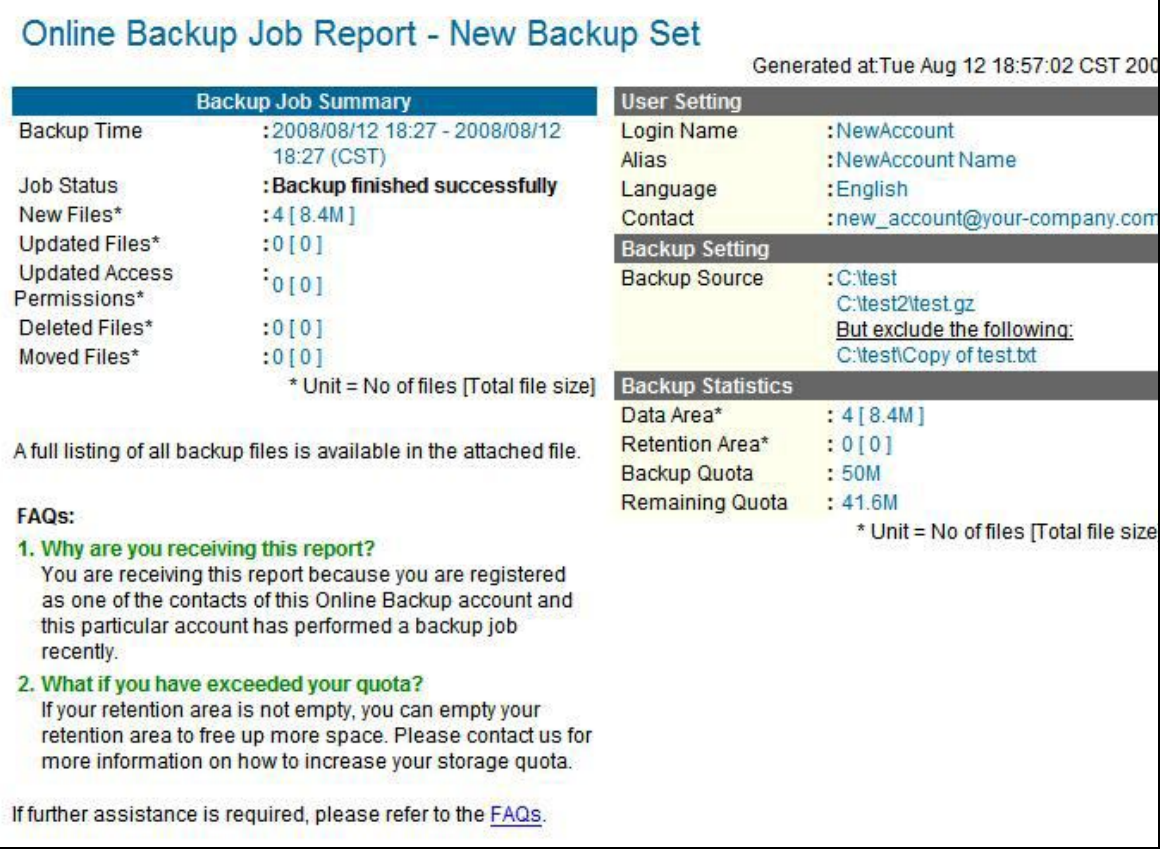
Sample Report

Request for forgotten password
Generated at: Tue Aug 12 18:21:45 CST 2008
FAQs:
1. Why are you receiving this report?
When a user visits the forgot password page and requests the password for this backup account, all registered contacts for this account will receive a password reminder email. If the password reminder was not requested by an authorized user, please contact us immediately.
2. What should you do after reading this email ?
Your current password is shown under the user setting. You are suggested to change your password to a more easily remembered password and delete this email to avoid any third party gaining your password.
User Setting
Login Name :NewAccount
Password :6ZoYxCjLONXyYlU2eJluAw==
Alias :NewAccount Name
Language :English
Contact :new_account@your-company.com

Key	Description
Login Name	**Login name**
Password	**Password**
Alias	**Alias**
Language	**Preferred Language for your backup report.**
Contact	**Email Address that will be used to contact you.**

21.3 Backup Job Report

For each backup job that you have run, a backup job report will be sent to you by email. This report contains a summary for the backup job that was run and a full listing of all files being backed up by the backup job. The backup summary report contains the following information:

Sample Backup Summary Report


Online Backup Job Report - New Backup Set

Generated at:Tue Aug 12 18:57:02 CST 200

Backup Job Summary

Backup Time	:2008/08/12 18:27 - 2008/08/12 18:27 (CST)
Job Status	:**Backup finished successfully**
New Files*	:4 [8.4M]
Updated Files*	:0 [0]
Updated Access Permissions*	:0 [0]
Deleted Files*	:0 [0]
Moved Files*	:0 [0]

* Unit = No of files [Total file size]

A full listing of all backup files is available in the attached file.

FAQs:

1. **Why are you receiving this report?**
   You are receiving this report because you are registered as one of the contacts of this Online Backup account and this particular account has performed a backup job recently.
2. **What if you have exceeded your quota?**
   If your retention area is not empty, you can empty your retention area to free up more space. Please contact us for more information on how to increase your storage quota.

If further assistance is required, please refer to the FAQs.

User Setting

Login Name	:NewAccount
Alias	:NewAccount Name
Language	:English
Contact	:new_account@your-company.com

Backup Setting

Backup Source	:C:\test C:\test2\test.gz But exclude the following: C:\test\Copy of test.txt

Backup Statistics

Data Area*	: 4 [8.4M]
Retention Area*	: 0 [0]
Backup Quota	: 50M
Remaining Quota	: 41.6M

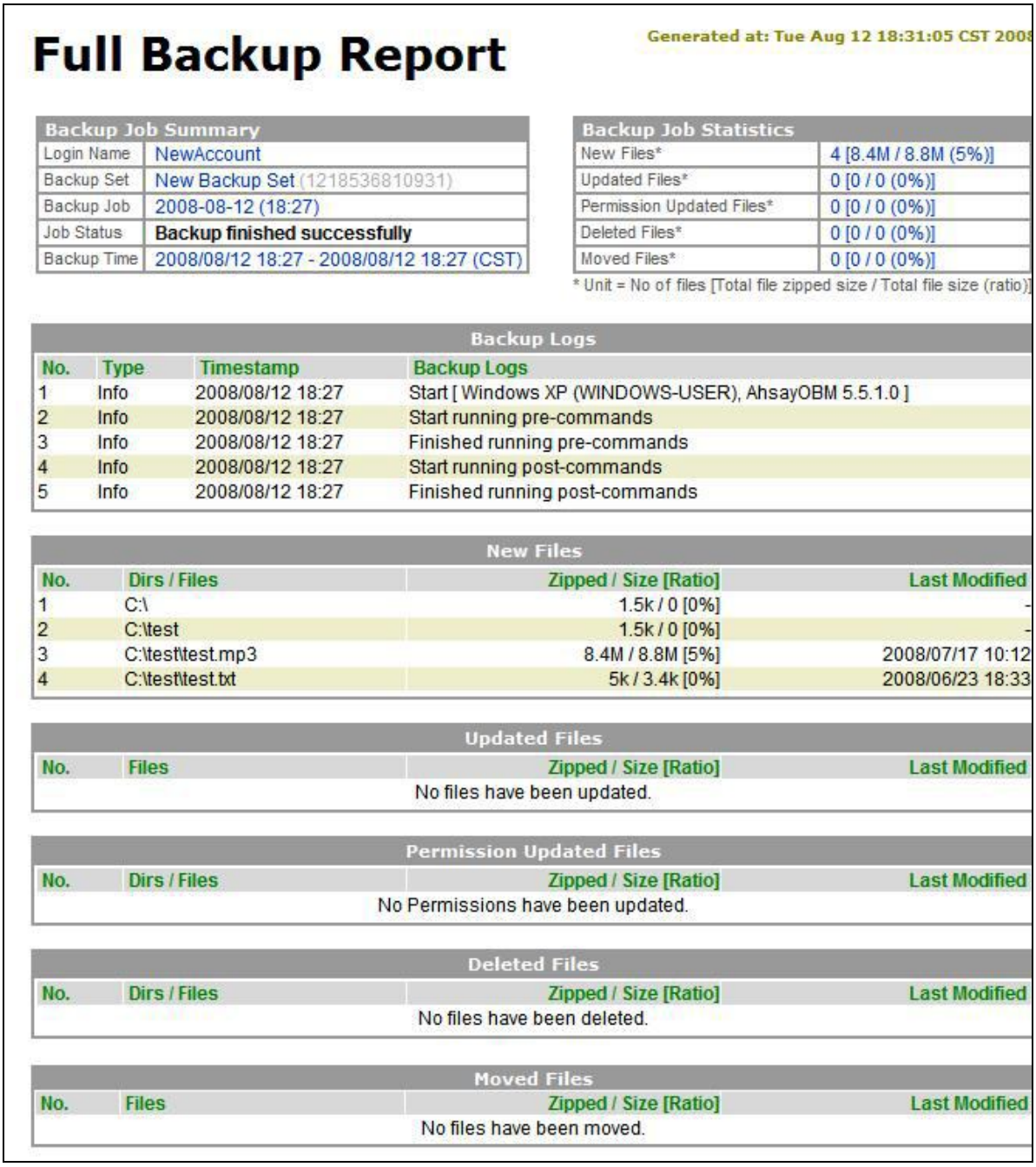
* Unit = No of files [Total file size

Key	Description
Login Name	Login name
Backup Time	The time when the backup job ran.
Job Status	The overall status of the backup job. Normally, you should see “Backup finished successfully" in this field. If you happen to get something else, please consult the attached full report for more information."
New Files	Total number and size of backup files added to your backup set.
Updated Files	Total number and size of backup files updated in your backup set.
Updated Access Permissions.	Total number and size of backup files with file permission updated in your backup set.
Deleted Files	Total number and size of backup files deleted from your backup set.
Moved Files	Total number and size of backup files relocated in your backup set.
Copied Files	Total number and size of backup files copied to another location in your backup set.
Login Name	Login Name

Alias	Alias
Language	Preferred Language for your backup report.
Contact	Email Address that will be used to contact you.
Backup Source	All files/directories that will be backed up.
Data Area	The total backup data stored in the data area.
Retention Area	The total backup data stored in the retention area. Old copies of updated or deleted backup files are retained in the retention area for the number of days as specified by the retention policy of the backup set before they are removed from the system.
Backup Quota	Backup quota
Remaining Quota	Remaining quota

The full backup report, which contains a full listing of all files backed up by the backup job, is attached to the backup job report email as a zip file. You need to unzip it before you can read the full report.

Sample Report



Full Backup Report

Generated at: Tue Aug 12 18:31:05 CST 200

Backup Job Summary	
Login Name	NewAccount
Backup Set	New Backup Set (1218536810931)
Backup Job	2008-08-12 (18:27)
Job Status	**Backup finished successfully**
Backup Time	2008/08/12 18:27 - 2008/08/12 18:27 (CST)

Backup Job Statistics	
New Files*	4 [8.4M / 8.8M (5%)]
Updated Files*	0 [0 / 0 (0%)]
Permission Updated Files*	0 [0 / 0 (0%)]
Deleted Files*	0 [0 / 0 (0%)]
Moved Files*	0 [0 / 0 (0%)]

* Unit = No of files [Total file zipped size / Total file size (ratio)]

Backup Logs

No.	Type	Timestamp	Backup Logs
1	Info	2008/08/12 18:27	Start [Windows XP (WINDOWS-USER), AhsayOBM 5.5.1.0]
2	Info	2008/08/12 18:27	Start running pre-commands
3	Info	2008/08/12 18:27	Finished running pre-commands
4	Info	2008/08/12 18:27	Start running post-commands
5	Info	2008/08/12 18:27	Finished running post-commands

New Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
1	C:\	1.5k / 0 [0%]	-
2	C:\test	1.5k / 0 [0%]	-
3	C:\test\test.mp3	8.4M / 8.8M [5%]	2008/07/17 10:12
4	C:\test\test.txt	5k / 3.4k [0%]	2008/06/23 18:33

Updated Files

No.	Files	Zipped / Size [Ratio]	Last Modified
No files have been updated.			

Permission Updated Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
No Permissions have been updated.			

Deleted Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
No files have been deleted.			

Moved Files

No.	Files	Zipped / Size [Ratio]	Last Modified
No files have been moved.			

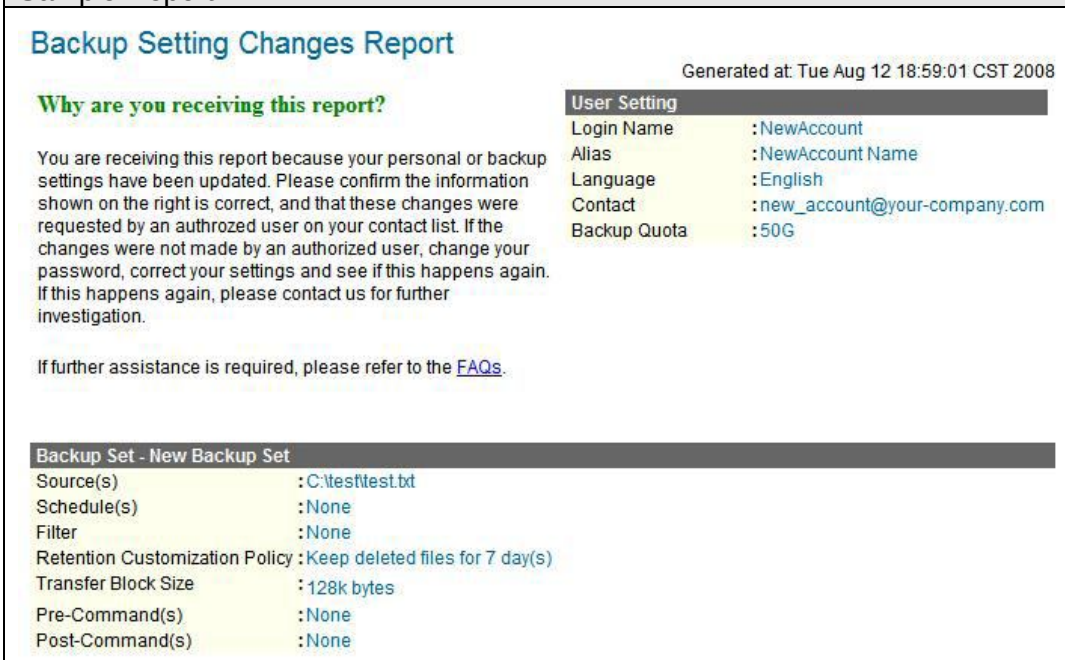
Key	Description
Backup Set	The name of the backup set.
Backup Job	The name of the backup job (which is the start time of the backup job).
Job Status	The overall status of the backup job. Normally, you should see “Backup finished successfully" in this field. If you happen to get something else, please consult the attached full report form more information.
Backup Time	The time when the backup job ran.
Backup Logs	All message logged when running this backup job.
New Files	Total number and size of backup files added to your backup set.
Updated Files	Total number and size of backup files updated in your backup set.

Permission Update Files	Total number and size of backup files with file permission updated in your backup set.
Deleted Files	Total number and size of backup files deleted from your backup set.
Moved Files	Total number and size of backup files relocated in your backup set.
Copied Files	Total number and size of backup files copied to another location in your backup set.
New File List	Full list of all backup files added to your backup set.
Updated File List	Full list of all backup files updated in your backup set.
Permission Updated File List	Full list of all backup files with file permission updated in your backup set.
Deleted File List	Full list of all backup files deleted from your backup set.
Moved File List	Full list of all backup files relocated in your backup set.
Copied File list	Full list of all backup files copied to another location in your backup set.

21.4 Setting Change Report

After you have updated your user profile or backup setting, a setting change report will be sent to you. This report allows you to track record of the changes that have been made to your backup account.

Sample Report



Backup Setting Changes Report

Generated at: Tue Aug 12 18:59:01 CST 2008

Why are you receiving this report?

You are receiving this report because your personal or backup settings have been updated. Please confirm the information shown on the right is correct, and that these changes were requested by an authrozed user on your contact list. If the changes were not made by an authorized user, change your password, correct your settings and see if this happens again. If this happens again, please contact us for further investigation.

If further assistance is required, please refer to the FAQs.

User Setting

Login Name	:NewAccount
Alias	:NewAccount Name
Language	:English
Contact	:new_account@your-company.com
Backup Quota	:50G

Backup Set - New Backup Set

Source(s)	:C:\test\test.txt
Schedule(s)	:None
Filter	:None
Retention Customization Policy	:Keep deleted files for 7 day(s)
Transfer Block Size	:128k bytes
Pre-Command(s)	:None
Post-Command(s)	:None

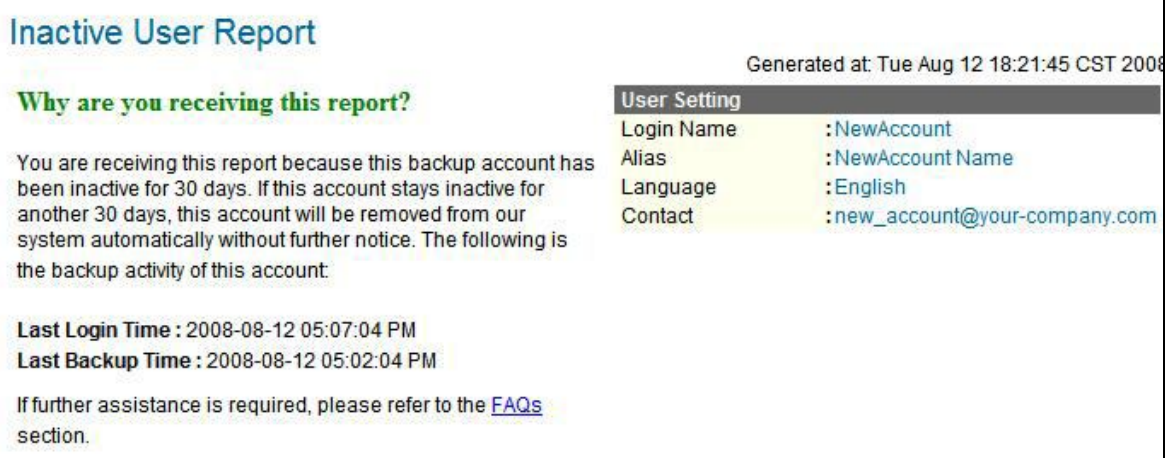
Key	Description
Login Name	Login Name
Alias	Alias
Language	Preferred Language for your backup reports
Contact	Email Address that will be used to contact you.
Backup Quota	Backup Quota
Source(s)	All backup sources of the backup set.
Schedule(s)	All backup schedules of the backup set.
Filter	All backup filters of the backup set.
Retention Customization Policy	The retention policy of the backup set.
Transfer Block Size	The transfer block size of the backup set.
Pre-Command(s)	All Pre-Command(s) of the backup set.
Post-Command(s)	All Post-Command(s) of the backup set.

21.5 Inactive User Reminder

You will receive an inactive user reminder in email if your account has been left inactive for the period of 7 days (or the period specified by the system administrator). This is to remind you that you have not been running backup for more than 7 days. If you are a

free trial user, your account will be removed from the system automatically if the system can track no records of your backup activities in the next 30 days after receiving this report.

Sample Report



Inactive User Report

Generated at: Tue Aug 12 18:21:45 CST 2008

Why are you receiving this report?

You are receiving this report because this backup account has been inactive for 30 days. If this account stays inactive for another 30 days, this account will be removed from our system automatically without further notice. The following is the backup activity of this account:

Last Login Time : 2008-08-12 05:07:04 PM
Last Backup Time : 2008-08-12 05:02:04 PM

If further assistance is required, please refer to the FAQs section.

User Setting	
Login Name	: NewAccount
Alias	: NewAccount Name
Language	: English
Contact	: new_account@your-company.com

Key	Description
Login Name	Login name
Alias	Alias
Language	Preferred Language for your backup reports.
Contact	Email Address that will be used to contact you.
Last Login Time	The last time you logon to the backup system.
Last Backup Time	The last time you ran a backup job.

22 Web Features

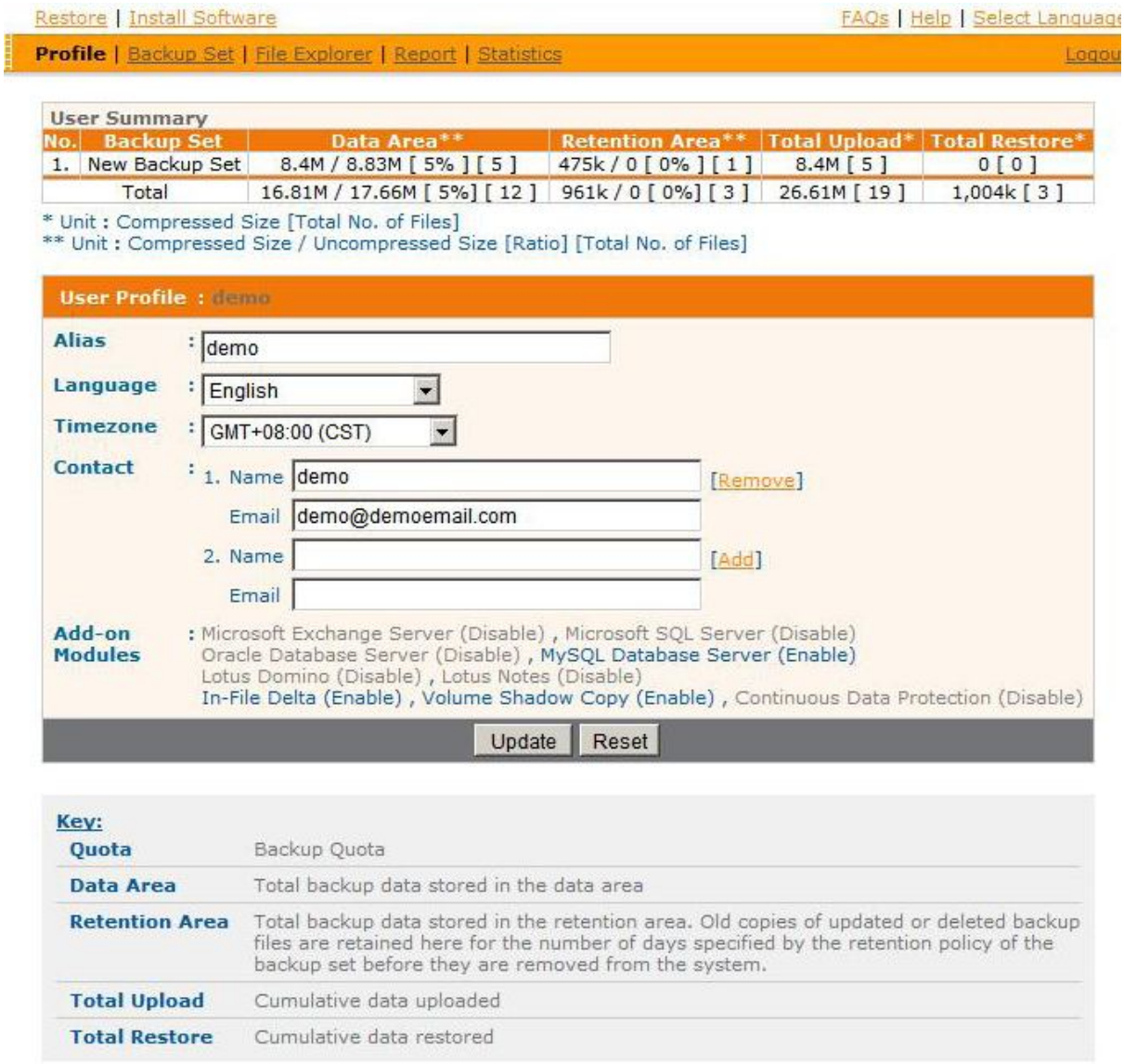
Other than the features of Quick Backup described in previous chapters, the web interface of Quick Backup Server provides you access to some additional features that are not available in Quick Backup. This chapter describes each of these features in details.

22.1 Install Quick Backup Software

Before you can use Quick Backup, you have to download the Quick Backup installer from the web interface of Quick Backup Server and install Quick Backup onto your computer. Please refer to the Installing Quick Backup section for information on how to install Quick Backup onto your computer.

22.2 Update User Profile

You can update your user profile by using the [Profile] panel available on the web interface. To change your profile, just make any changes to your profile on the panel shown below and press the [Update] button.


Restore | Install Software
FAQs | Help | Select Language
Profile | Backup Set | File Explorer | Report | Statistics
Logou
User Summary
No. Backup Set Data Area** Retention Area** Total Upload* Total Restore*
1. New Backup Set 8.4M / 8.83M [5%] [5] 475k / 0 [0%] [1] 8.4M [5] 0 [0]
Total 16.81M / 17.66M [5%] [12] 961k / 0 [0%] [3] 26.61M [19] 1,004k [3]
* Unit : Compressed Size [Total No. of Files]
** Unit : Compressed Size / Uncompressed Size [Ratio] [Total No. of Files]
User Profile : demo
Alias : demo
Language : English
Timezone : GMT+08:00 (CST)
Contact : 1. Name demo [Remove]
Email demo@demoemail.com
2. Name [Add]
Email
Add-on Modules : Microsoft Exchange Server (Disable) , Microsoft SQL Server (Disable)
Oracle Database Server (Disable) , MySQL Database Server (Enable)
Lotus Domino (Disable) , Lotus Notes (Disable)
In-File Delta (Enable) , Volume Shadow Copy (Enable) , Continuous Data Protection (Disable)
Update Reset
Key:
Quota Backup Quota
Data Area Total backup data stored in the data area
Retention Area Total backup data stored in the retention area. Old copies of updated or deleted backup files are retained here for the number of days specified by the retention policy of the backup set before they are removed from the system.
Total Upload Cumulative data uploaded
Total Restore Cumulative data restored

Key	Description
Quota	Backup quota
Data Area	Total number and size of backup files stored in the data area.
Retention Area	Total number and size of backup files stored in the retention area.
Total Upload	Total number and size of backup files uploaded to the backup server.
Total Restore	Total number and size of backup files restored from the backup server.
Login Name	Login name.
Alias	Display Name of your backup account.
Language	Preferred Language for your backup report.

Time Zone	Your Time zone.
Contact	Email Address that will be used to contact you.

22.3 Request Forgotten Password

If you have forgotten your password, you can retrieve it by simply entering your login name or your registered email address on the [Password Request] form and press the [Request] button. Your password will be sent to your registered email address automatically.

22.4 Restore/Delete/Undelete Backup Files

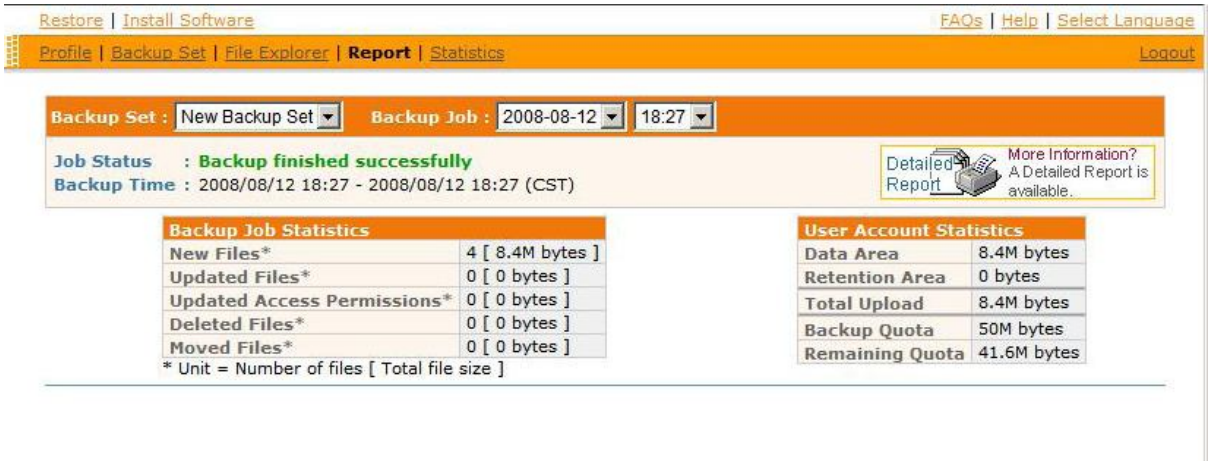
Using the [File Explorer], you can browse through the backup data (both current and previous versions) on Quick Backup Server. You can select any current backup files to Restore or Delete. You can also select any deleted backup files (in gray) to Undelete.

Note: Restore of native features, e.g. file attribute/file permission/symbolic links/junction points are not supported by the Web Restore Applet.

Restore | Install Software
FAQs | Help | Select Language
Profile | Backup Set | File Explorer | Report | Statistics
Logout
Rows/Page: 50
Home > New Backup Set > C:\ > test
Show files As Of 2008-08-12 18:27
Show all files
Show Jobs View
Show Advanced Option
Delete
Restore
File / Directory
Size
Last Modified
Zipped [Ratio]
..
test.mp3
8.82M
2008/07/17 10:12
8.39M [4%]
test.txt
3k
2008/06/23 18:33
3k [0%]
Delete
Restore
Note:
1. This shows all files / directories within a backup job of a backup set.
2. Files shown in light gray color are retained in the retention area.
3. To restore files/directories, check the checkbox next to the files/directories and press the [Restore] button.
4. To delete files/directories, check the checkbox next to the files/directories and press the [Delete] button.
5. [D] = Differential delta file
6. [I] = Incremental delta file

22.5 Review Backup Jobs

In addition to reviewing your backup activities from the email report and from Quick Backup, you can also review any of your backup jobs by using the [Report] panel available on the web interface. To review a backup job, select the required backup job from the [Backup Set] and [Backup Job] drop-down lists.


Restore | Install Software
FAQs | Help | Select Language
Profile | Backup Set | File Explorer | Report | Statistics
Logout
Backup Set : New Backup Set
Backup Job : 2008-08-12 18:27
Job Status : Backup finished successfully
Backup Time : 2008/08/12 18:27 - 2008/08/12 18:27 (CST)
Detailed Report
More Information? A Detailed Report is available.
Backup Job Statistics
New Files* 4 [8.4M bytes]
Updated Files* 0 [0 bytes]
Updated Access Permissions* 0 [0 bytes]
Deleted Files* 0 [0 bytes]
Moved Files* 0 [0 bytes]
* Unit = Number of files [Total file size]
User Account Statistics
Data Area 8.4M bytes
Retention Area 0 bytes
Total Upload 8.4M bytes
Backup Quota 50M bytes
Remaining Quota 41.6M bytes

Key	Description
Job Status	The overall status of the backup job. Normally, you should see “Backup finished successfully" in this field. If you happen to get something else, please click the [Detailed Report] image on the page.
Backup Time	The time when the backup job ran.
New Files	Total number and size of backup files added to your backup set.
Updated Files	Total number and size of backup files updated in your backup set.
Updated Access Permissions	Total number and size of backup files with file permission updated in your backup set.
Deleted Files	Total number and size of backup files deleted from your backup set.
Moved Files	Total number and size of backup files relocated in your backup set.
Copied Files	Total number and size of backup files copied to another location in your backup set.
Data Area	The total backup data stored in the data area.
Retention Area	The total backup data stored in the retention area. Old copies of updated or deleted backup files are retained in the retention area for the number of days as specified by the retention policy of the backup set before they are removed from the system
Total Upload	Total number and size of backup files uploaded to the backup server.
Backup Quota	Backup Quota
Remaining Quota	Remaining Quota

You can open the [Full Backup Report] to review all information logged by a backup job by clicking the [Detailed Report] image on the [Report] panel.

Full Backup Report

Backup Job Summary	
Login Name	QBDemo
Backup Set	Data (1318979790727)
Backup Job	2011-10-19 (14:00)
Job Status	Backup finished successfully
Backup Time	2011/10/19 13:59 - 2011/10/19 14:00 (EST)

Backup Job Statistics	
New Files*	6 [38.6k / 14.7M (100%)]
Updated Files*	0 [0 / 0 (0%)]
Permission Updated Files*	0 [0 / 0 (0%)]
Deleted Files*	9 [380k / 409.7k (7%)]
Moved Files*	3 [376.1k / 467.7k (20%)]

* Unit = No of files [Total file zipped size / Total file size (ratio)]

Backup Logs

No.	Type	Timestamp	Backup Logs
1	Info	2011/10/19 13:59	Start [Windows 7 (C:PC), Quick Backup Enterprise Edition 6.7.0.0
2	Info	2011/10/19 13:59	Using Temporary Directory C:\Users\Joe\.temp
3	Info	2011/10/19 13:59	Start running pre-commands
4	Info	2011/10/19 13:59	Finished running pre-commands
5	Info	2011/10/19 13:59	Start creating Shadow Copy Set ...
6	Info	2011/10/19 13:59	Shadow Copy Set successfully created
7	Info	2011/10/19 14:00	Deleting Shadow Copy snapshot for volume "D:\"
8	Info	2011/10/19 14:00	Start running post-commands
9	Info	2011/10/19 14:00	Finished running post-commands

New Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
1	D:\Data\Archived Data\Old Banking	1.5k / 0 [0%]	-
2	D:\Data\Expenses	1.5k / 0 [0%]	-
3	D:\Data\Accounts Data\Banking\NAB	1.5k / 0 [0%]	-
4	D:\Data\Accounts Data\Banking\NAB\nab.mdb	7.1k / 2.8M [100%]	2011/09/09 13:45
5	D:\Data\Expenses\exps.xls	4k / 1.2M [100%]	2011/09/09 13:33
6	D:\Data\Compliance\file7.xls	23k / 10.7M [100%]	2011/09/09 13:33

Updated Files

No.	Files	Zipped / Size [Ratio]	Last Modified
No files have been updated.			

Permission Updated Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
No Permissions have been updated.			

Deleted Files

No.	Dirs / Files	Zipped / Size [Ratio]	Last Modified
1	D:\Data\Logos & Graphics\company_banner.gif	8.1k / 6.6k [0%]	2007/06/15 23:10
2	D:\Data\Logos & Graphics\Final Logo.JPG	202.1k / 234.4k [14%]	2006/08/11 11:43
3	D:\Data\Logos & Graphics\Logo.gif	8.7k / 7.1k [0%]	2006/10/08 21:39
4	D:\Data\Logos & Graphics\Logo_Doco.jpg	111.4k / 119.2k [7%]	2006/08/11 11:45
5	D:\Data\Logos & Graphics\company_splashscreen.gif	17.9k / 16.4k [0%]	2007/06/15 23:04
6	D:\Data\Logos & Graphics\company_splashScreen1.gif	17.4k / 15.9k [0%]	2007/05/28 22:52
7	D:\Data\Logos & Graphics\Logo_EmailReports.gif	4.3k / 2.7k [0%]	2007/04/29 18:36
8	D:\Data\Logos & Graphics\Logo_Sig.jpg	8.6k / 7.4k [0%]	2006/11/04 17:53
9	D:\Data\New folder	1.5k / 0 [0%]	-

Moved Files

No.	Files	Zipped / Size [Ratio]	Last Modified
1	D:\Data\Accounts Data\Banking\2006_Fees_&_Charges.pdf -> D:\Data\Archived Data\Old Banking\2006_Fees_&_Charges.pdf	76.4k / 99.7k [23%]	2006/07/21 12:18
2	D:\Data\Accounts Data\Banking\2006_OPS_Merchant_Business_Plan.doc -> D:\Data\Archived Data\Old Banking\2006_OPS_Merchant_Business_Plan.doc	185.6k / 234.5k [21%]	2006/07/21 13:16
3	D:\Data\Accounts Data\Banking\2006_T&Cs.pdf -> D:\Data\Archived Data\Old Banking\2006_T&Cs.pdf	114.2k / 133.5k [14%]	2006/07/21 12:18

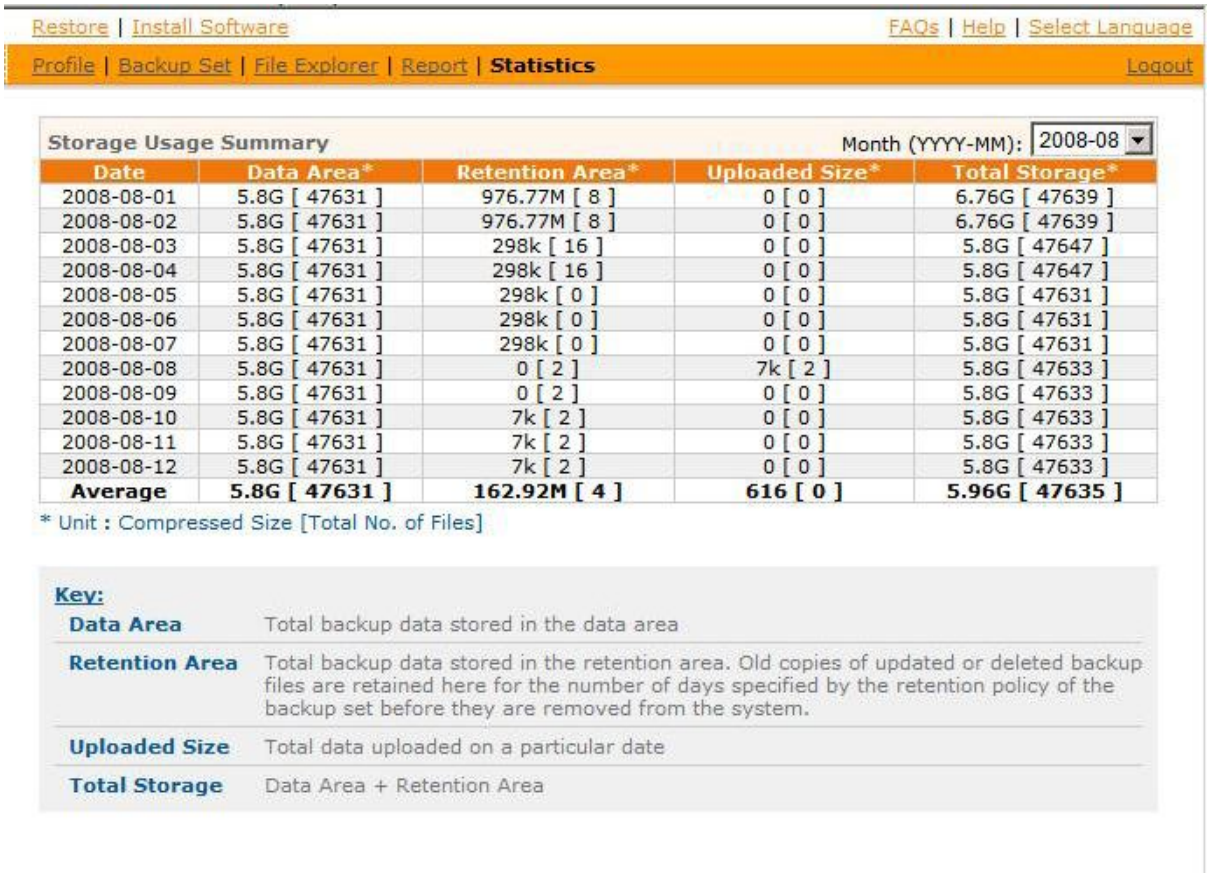
Note: This report shows all information recorded for this backup job

Key	Description

Login Name	The login name of the user.
Backup Set	The name of the backup set.
Backup Job	The name of the backup job (which is the start time of the backup job).
Job Status	The overall status of the backup job.
Backup Time	The time when the backup job ran.
Backup Logs	All messages logged when running this backup job.
New Files	Total number and size of backup files added to your backup set.
Updated Files	Total number and size of backup files updated in your backup set.
Permission Updated Files	Total number and size of backup files with file permission updated in your backup set.
Deleted Files	Total number and size of backup files deleted from your backup set.
Moved Files	Total number and size of backup files relocated in your backup set.
Copied Files	Total number and size of backup files copied to another location in your backup set.
New File List	Full list of all backup files added to your backup set.
Updated File List	Full list of all backup files updated in your backup set.
Permission Updated File List	Full list of all backup files with file permission updated in your backup set.
Deleted File List	Full list of all backup files deleted from your backup set.
Moved File List	Full list of all backup files relocated in your backup set.
Copied File List	Full list of all backup files copied to another location in your backup set.

22.6 Review Storage Statistics

You can review the amount of data you have stored on the backup server and uploaded to the backup server on each day by opening the [Statistics] panel available on the web interface. To review your storage statistics for a different month, just select the month from the [Month] drop-down list.


Restore | Install Software
FAQs | Help | Select Language
Profile | Backup Set | File Explorer | Report | Statistics
Logout
Storage Usage Summary
Month (YYYY-MM): 2008-08
Date | Data Area* | Retention Area* | Uploaded Size* | Total Storage*
2008-08-01 | 5.8G [47631] | 976.77M [8] | 0 [0] | 6.76G [47639]
2008-08-02 | 5.8G [47631] | 976.77M [8] | 0 [0] | 6.76G [47639]
2008-08-03 | 5.8G [47631] | 298k [16] | 0 [0] | 5.8G [47647]
2008-08-04 | 5.8G [47631] | 298k [16] | 0 [0] | 5.8G [47647]
2008-08-05 | 5.8G [47631] | 298k [0] | 0 [0] | 5.8G [47631]
2008-08-06 | 5.8G [47631] | 298k [0] | 0 [0] | 5.8G [47631]
2008-08-07 | 5.8G [47631] | 298k [0] | 0 [0] | 5.8G [47631]
2008-08-08 | 5.8G [47631] | 0 [2] | 7k [2] | 5.8G [47633]
2008-08-09 | 5.8G [47631] | 0 [2] | 0 [0] | 5.8G [47633]
2008-08-10 | 5.8G [47631] | 7k [2] | 0 [0] | 5.8G [47633]
2008-08-11 | 5.8G [47631] | 7k [2] | 0 [0] | 5.8G [47633]
2008-08-12 | 5.8G [47631] | 7k [2] | 0 [0] | 5.8G [47633]
Average | 5.8G [47631] | 162.92M [4] | 616 [0] | 5.96G [47635]
* Unit : Compressed Size [Total No. of Files]
Key:
Data Area
Total backup data stored in the data area
Retention Area
Total backup data stored in the retention area. Old copies of updated or deleted backup files are retained here for the number of days specified by the retention policy of the backup set before they are removed from the system.
Uploaded Size
Total data uploaded on a particular date
Total Storage
Data Area + Retention Area

Key	Description
Date	The date that the following statistics are collected.
Data Area	Total number and size of backup files stored in the data area on a particular date.
Retention Area	Total number and size of backup files stored in the retention area on a particular date.
Uploaded Size	Total number and size of backup files uploaded to the backup server on a particular date.
Total Storage	Total number and size of backup files stored under your backup account on a particular date.

23 Further Information

23.1 Contact Us

For current customers take a look in our Support knowledge base and Technical FAQs area to find instant answers or submit a Quick Support request to contact us

Phone: 02 8094 1245

Email: support@quickbackup.com.au

You can find our contact information by following instructions below.

1. Open Quick Backup from system tray.
2. Click the button from the menu.
3. Contact us by using the information shown in the [About] dialog box.

Appendix

Appendix A Supported Languages

Language Code	Language
de	German
en	English
el	Spanish
fr	French

Appendix B Website location

www.quickbackup.com.au